16th INTERNATIONAL CONFERENCE

24 - 26 MAY 2023 BRUSSELS, BELGIUM

COMPUTERS, PRIVACY & DATA PROTECTION

CPDP2023

IDEAS THAT DRIVE OUR DIGITAL WORLD

WWW.CPDPCONFERENCES.ORG

16th INTERNATIONAL CONFERENCE
24 - 26 MAY 2023 BRUSSELS, BELGIUM
COMPUTERS, PRIVACY & DATA PROTECTION

CPDP2023
IDEAS THAT DRIVE OUR DIGITAL WORLD

VUB LSTS LAW, SCIENCE, TECHNOLOGY & SOCIETY RESEARCH GROUP

Inria informatics mathematics

Tilt Tilburg Institute for Law, Technology, and Society

Fraunhofer ISI

ALTI

CEU Universidad San Pablo

CRISP CENTRE FOR RESEARCH INTO INFORMATION, SURVEILLANCE & PRIVACY

cordellinstitute.wustl.edu

eLAW LEIDEN

FGV DIREITO RIO

FIZ Karlsruhe Leibniz Institute for Information Infrastructure

Georgia Tech College of Computing School of Cybersecurity and Privacy

HCLT המרכז למשפט וטכנולוגיה The Haifa Center for Law & Technology

IVIR

KU LEUVEN CiTiP CENTRE FOR IT & IP LAW

The Ohio State University PROGRAM ON DATA AND GOVERNANCE

dg Università di Torino Dipartimento di Giurisprudenza

uni.lu UNIVERSITÉ DU LUXEMBOURG

WEDNESDAY 24TH MAY 2023

Please note that this is a preliminary version of the programme.

24.5	GRANDE HALLE	AREA 42 GRAND	AREA 42 MIDI
7.30	Registration in La Cave	Registration in La Cave	Registration in La Cave
8.30	Welcome and Introduction by Paul De Hert	Welcome and Introduction in Grande Halle	Welcome and Introduction in Grande Halle
8.45	Global AI Governance: Policy and Practice organised by International Association of Privacy Professionals (IAPP) Page 17	Exploring the many faces of the GDPR- in search of effective data protection regulation organised by Haifa Center for Law and Technology Page 19	Measuring dark patterns and their harms: a multidisciplinary, anticipatory perspective organised by SnT, University of Luxembourg Page 21
10.00	Coffee break		
10.30	What will change in 2024? organised by Council of Europe Page 17	Reforming the online adtech ecosystem: options for change beyond the e-privacy directive, DSA and DMA organised by AWO Agency Page 19	Data Protection Authorities in Emergencies organised by CPDP Page 22
11.45	Does the computer know I am a child? Protecting child rights in an age of algorithms. organised by FRA Page 17	A Market of One: Personalised pricing from a data, competition and consumer protection perspective organised by BEUC Page 20	Addressing the digital divide to achieve equal and inclusive healthcare in Europe organised by TILT Page 22
13.00	Lunch	13.00 Chat control: lurking surveillance state? by Privacy Platform Page 20	
14.15	Dialogue on Friction Between Modern Marketing and Advertising and GDPR and ePrivacy Directive: Is There an Effective Way Forward? organised by Interpublic Group Page 18	14.15 Model Clauses Go Global: EU-Asean Cooperation organised by European Commission Page 20	Vulnerable who? Vulnerable when? Vulnerable to what? organised by VULNERA, the International Observatory Page 22
15.30	Coffee break		
16.00	Examining Fundamental Rights in a New Era of AI organised by Microsoft Page 18	From notorious rule breaker to privacy advocate: how government can change its stripes organised by Bits of Freedom Page 20	Duties of Data Loyalty and the Future of Data Protection organised by Washington University Page 23
17.15	Moving towards a Sustainable and Functional EU-US Transfers Framework? organised by CPDP Introductory Remarks by European Commissioner for Justice, Didier Reynders Page 18	Looking beyond the EU data strategy: where next for data use and regulation? organised by Ada Lovelace Institute Page 21	From theory to the practice: digital constitutionalism and data justice in movement in the Global South organised by Data Privacy Brasil Research Association Page 23
18.30	Cocktail sponsored by EDPS in Le Village		

LA CAVE	AREA 42 PETIT	M-VILLAGE GRANDE	M-VILLAGE MIDI
Registration in La Cave	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	Welcome and Introduction in Grande Halle
Youth Privacy Protection and Online Gaming organised by Université de Paris-Saclay and INSA Centre Val de Loire Page 24	How to Determine the Right Anonymisation Measures if the Term "Personal Data" is Unclear? Finding the Missing Pieces for a Functional Anonymisation Framework by Einstein Center Digital Future, Berlin University of the Arts Page 26	Workshop When data privacy meets corporate morality: should data protection be part of corporate social responsibility? organised by CMS Page 28	Workshop Internet shutdowns - are internet blackouts ever justified? organised by LSTS Page 30
Coffee break			
Chronicle of a Death Foretold: Is EU predictive security policy killing Data Protection? organised by Free Group Page 24	Blockchain-based identity management systems: Opportunities and Challenges organised by CiTiP, KU Leuven Page 26	Workshop Advanced Data Protection Control (ADPC): A Fundamental Transformation in Privacy Practices by Sustainable Computing Lab, Vienna University of Economics and Business Page 28	Workshop Trustworthy (re)use of health data endorsed by EHDS organised by The European Institute for Innovation through Health Data (i~HD) Page 30
AI Act for all people? Interrogating Europe's AI regulation from the migration perspective organised by EDRi Page 24	How to make privacy more user-friendly for the long-term organised by EPFL Center for Digital Trust and UC Berkeley Center for Long-Term Cybersecurity Page 26	Workshop The (Artificial) Right to Effective Remedy: Effective Remedy and Citizen Complaints Revisited organised by AI 4 Belgium Page 28	Workshop How to design and use privacy icons to effectively inform about privacy risks organised by University of the Arts Berlin / Einstein Center Digital Future Page 30
Lunch			
Non-Compulsory Government Access to Data: the Next Frontier for Surveillance Reform? organised by Stiftung Neue Verantwortung Page 25	The EHDS and secondary use of data: is it possible to balance individual interests with the ultimate need for data sharing to facilitate research? organised by Vrije Universiteit Brussel, Health and Ageing Law Lab (LSTS, HALL) Page 27	Workshop Automated enforcement of the GDPR and other digital rights-can legal tech be a solution? organised by NOYB Page 29	Workshop Tensions Between Consumer Law and Privacy in the Content Creator Economy organised by Utrecht University/UU Page 30
Coffee break			
Interoperability in the EU's AFSJ: preparing to supervise the "point of no return" organised by European Data Protection Supervisor Page 25	Dignity, Technology and Human Values in Smart Technological Environments: From Design to the Lived Experience by Center for Research into Information, Surveillance and Privacy Page 27	Workshop Data protection in the EU Regulation on Political Advertising: a new paradigm? organised by European Partnership for Democracy (EPD) Page 29	Workshop Personalised Privacy: How can we Leverage Personalisation for Better Privacy Protection? organised by Maastricht University, Law and Tech Lab Page 31
Shine a Light: Data Protection and Law Enforcement in the Digital Age organised by Europol Data Protection Experts Network (EDEN) Page 25	Who is visible in data protection? An anti-racist perspective for tech organised by European Network Against Racism (ENAR) Page 27	Workshop Right to Digital Integrity - a New Framework for Data Portection organised by Nym Technologies Page 29	Workshop World Cafe: Whose Data? The New Individual and New Collective in the Digital-World organised by University of Manchester Page 31
Cocktail sponsored by EDPS in Le Village			

THURSDAY 25TH MAY 2023

Please note that this is a preliminary version of the programme.

25.5	GRANDE HALLE	AREA 42 GRAND	AREA 42 MIDI
7.30	Registration in La Cave	Registration in La Cave	Registration in La Cave
8.45	Best Practices for Protecting Children's Privacy in the Digital Age: the Practitioners' Perspective organised by CPDP Page 32	Sharing is caring: data intermediaries, synthetic data and best practices for data spaces organised by Centro Nazionale IoT e Privacy Page 34	Bridging the gap – enforcing the DMA, learning from the data protection experience organised by ARTICLE 19 Page 36
10.00	Coffee break		
10.30	Is strong encryption more important now than ever? organised by Apple Page 32	Trustworthy data spaces from the perspective of their developers and users - current challenges and the way forward organised by Department of Innovation and Digitalisation in Law, University of Vienna Page 34	New EU digital legislation and its impact on the role of Supervisory Authorities and DPOs organised by European Federation of Data Protection Officers Page 36
11.45	Convergence in action: cooperation through networks – from the regional to the global dimension organised by European Commission Page 32	Regulating e-Mental Health: Progress, Pitfalls and Global Lessons organised by IEEE Standards Association Page 34	How democracies protect both privacy and national security organised by American University Page 36
13.00	Lunch		
14.15	The Future of Effective Enforcement organised by European Data Protection Supervisor Page 33	Privacy Engineering for Transparency and Accountability organised by TU Berlin Page 35	(Mis)use of surveillance technologies as emergency measures: global lessons from the Covid-19 pandemic organised by International Network of Civil Liberties Organizations Page 37
15.30	CNIL-Inria Privacy Award & EPIC Champion of Freedom Award		
16.00	Privacy through Innovation - Privacy Enhancing Technologies, Consumer Protection and the Online Ads Ecosystem organised by Google Page 33	The Underuse of Personal Data, Its Opportunity Costs, and EU Policies organised by University of Turin Page 35	When Privacy Becomes Political organised by Datatilsynet Page 37
17.15	AI Fairness Testing: Making It Work in the Real World organised by Uber Page 33	Connecting global privacy frameworks to enable trusted data flows organised by Workday Page 35	Deceptive design in online interfaces and system architecture: questions for EU law organised by Vrije Universiteit Amsterdam Page 37
18.30	Cocktail sponsored by Uber in Le Village		

LA CAVE	AREA 42 PETIT	M-VILLAGE GRANDE	M-VILLAGE MIDI
Registration in La Cave	Registration in La Cave	Registration in La Cave	Registration in La Cave
Guardians of Ethical AI organised by KU Leuven Digital Society Institute Page 38	Addressing Risks in Emerging Legislative Initiatives and Engineering Data Protection (and Security) Measures organised by ENISA Page 40	Workshop Data Autonomy In Higher Education: The Quest For 'Public Values In The Cloud' organised by University of Groningen Page 42	Working & Meeting Space Page 44
Coffee break			
The global harms of powering Artificial Intelligence – Towards a sustainable future of data use and governance organised by AlgorithmWatch Page 38	Technical Standards and the AI Act: Legitimate and Sufficient? organised by ADAPT Centre at Trinity College Dublin Page 40	Workshop GDPR Certification in Practice organised by Mandat International Page 42	Workshop Privacy Threat Modeling for AI systems organised by Rhite Page 44
organised by Mozilla Page 38	Enforcement of Data Protection by Design & by Default: consequences for the uptake of Privacy-Enhancing Technologies in the EU organised by Future of Privacy Forum Page 41	Roundtable "It's not about the personal data, stupid! Is it time to focus legal protection against risks of the digital society on something else?" organised by ERC INFO-LEG project, Utrecht University Page 43	Workshop Inclusive co-design and societal acceptance of emerging security technologies: ambitions and best practices organised by Centre for IT & IP Law, KU Leuven Page 44
Press conference of the European Data Protection Board (at lunch in La Cave) Page 38			
Regulating accountability in complex AI value chains: research collaboration, text and data mining, and other possible traps organised by Microsoft Page 39	Preparing Cryptography for the Quantum Age organised by Quantum Software Consortium Page 41	Workshop State-of-play of Privacy-Preserving Machine Learning (PPML) - auditing bias, mitigating privacy risks in ML-systems organised by Future of Privacy Forum Page 43	Working & Meeting Space Page 45
Coffee break			
Assessing the Impact of [Algorithmic] Impact Assessments organised by EPIC Page 39	EDPL Young Scholar Award organised by Lexxion Publisher Page 41	Workshop Future Trend: the Conflict between Cybersecurity and Privacy organised by Deloitte Page 43	Workshop The UK's approach to International Data Transfers: How to build trust, deliver growth and fire up innovation organised by Department for Science, Innovation and Technology (DSIT), UK Page 45
E-Commerce and Data Transfers: A Latin American Perspective organised by Center for Technology and Society at FGV and the European Commission Page 39	GDPR automation: Might the law (unintentionally) push towards automation? organised by LSTS, Vrije Universiteit Brussel (VUB) Page 42	Workshop The State of Data Protection Law Academia organised by Data Protection Law Scholars' Network (DPSN) Page 44	Workshop Moot Court: The value of health data organised by Department of Innovation and Digitalisation in Law, University Vienna Workshop Page 45
BRICS Panel Page 40	Cocktail sponsored by Uber in Le Village		

FRIDAY 26TH MAY 2023

Please note that this is a preliminary version of the programme.

26.5	GRANDE HALLE	AREA 42 GRAND	AREA 42 MIDI
7.30	Registration in La Cave	Registration in La Cave	Registration in La Cave
8.45	See You in Court! organised by NOYB Page 46	Beyond ethics washing. Impact assessments, audits, and oversight for AI organised by Helsinki Institute for Social Science and Humanities, University of Helsinki Page 48	Dark patterns: definitions and evidence for regulators organised by INRIA Page 50
10.00	Coffee break		
10.30	Fairness in Personalisation: the Role of Transparency, User Control, and the Balance between Fundamental Rights organised by Meta Page 46	Whose digital future? Engaging citizens in AI development and impact assessment organised by European Center for Not-for-Profit Law (ECNL) Page 48	Increased government access to personal data: Rethinking the roles of citizens and the private sector organised by Academia Sinica Page 50
11.45	The Collection, Sharing, and Use of Gender Data organised by Northeastern University Page 46	Have you tried asking? Engaging with citizens in policy and product development organised by Information Commissioner's Office Page 48	The New E-Evidence Regulation: Problem Solved or Opening of a Pandora's box? organised by University of Luxembourg Page 50
13.00	Lunch		
14.15	Subjects and Structures: Re-Imagining Data Protection as a Critique of Power organised by Fraunhofer ISI Page 47	The Social and Ethical Implications of Implantable Enhancement Technology organised by Centre for Business Information Ethics, Meiji University Page 48	Will the Digital Services Act promote safer and healthier algorithmic rankings? organised by The Mozilla Foundation Page 51
15.30	Coffee break		
16.00	A Safe Space to Create - How Platforms Are Approaching Minor Privacy organised by TikTok Page 47	The Changing Face of Consumer Protection in Africa's Digital Economy organised by Lawyers Hub Page 49	The regulation of online advertising, between the GDPR and the DSA organised by IVIR – DSA Observatory, University of Amsterdam Page 51
17.15	The End of Online Behavioural Advertising organised by Leiden University Page 47	GDPR & LGPD: Exploring the Potential of Codes of Conduct Across Borders organised by Scope Europe Page 49	The Governance of AI: Convergence or Divergence? organised by Center for AI and Digital Policy Page 51
18.30	Closing remarks by Wojciech Wiewiórowski and Christopher Kuner	Closing remarks in Grande Halle	Closing remarks in Grande Halle
19.00	Cocktail sponsored by Privacy Salon in Le Village		

LA CAVE	AREA 42 PETIT	M-VILLAGE GRANDE	M-VILLAGE MIDI
Registration in La Cave	Registration in La Cave	Registration in La Cave	Registration in La Cave
Accountability tools: from transfers to cross-border interoperability organised by Center for Information and Policy Leadership Page 52	Achieving social justice for data workers: is there a role for harmonised standards? organised by European Trade Union Institute Page 54	Workshop How to bring Control back to the humans beings -Enlightening the AI black box organised by nexus Institut Berlin Page 56	Seminar Philosophers' Seminar on Compliance and Automation in Data Protection Law organised by CPDP, ALTEP-DP and COHUBICOL (BE) Page 57
Coffee break			
EU-US Data Privacy Framework: How does the US EO Sustain a new Durable Agreement? organised by CEU San Pablo University – South EU Google Data Governance Chair Page 52	Academic Session 1 organised by CPDP speakers Amir Cahane, Hebrew University of Jerusalem (IL); Shrutika Gandhi, Institute of Advanced Legal Studies, University of London (UK); Audrey Dequesness, University of Lille (FR) Page 55	Book Launch "Vulnerability and Data Protection Law" Book Launch organised by "VULNERA" Observatory at the Brussels Privacy Hub Page 56	Seminar Philosophers' Seminar on Compliance and Automation in Data Protection Law organised by CPDP, ALTEP-DP and COHUBICOL (BE) Page 57
"Flexibility" in the "Essential Equivalence" Test For Data Transfers: Taking Into Account Different Legal Traditions and Constitutional Constraints in Third Countries organised by The School of Cybersecurity & Privacy, Georgia Institute of Technology Page 53	Academic Session 2 organised by CPDP speakers Julia Krämer, Erasmus University Rotterdam (NL); Klaudia Majcher, Vienna University of Economics and Business (AT) and Vrije Universiteit Brussel (BE); Jan Czarnocki, KU Leuven (BE); Karlo Lukic and Bernd Skiera, Goethe University Frankfurt (DE), and Klaus Miller, HEC Paris (FR) Page 55	Workshop Dark Patterns Fighters - Unite! organised by SnT, University of Luxembourg Page 56	Seminar Philosophers' Seminar on Compliance and Automation in Data Protection Law organised by CPDP, ALTEP-DP and COHUBICOL (BE) Page 57
Lunch			
Ending the privacy of those who are supposed to be protected or effectively safeguarding children against online sexual abuse? organised by European Centre on Privacy and Cybersecurity (ECPC) Page 53	Academic Session 3 organised by CPDP speakers Emmanouil Bougiakiotis, European University Institute (IT); Merel Noorman, Tilburg University (NL) and Tsjalling Swierstra, Maastricht University (NL); Ero Balsa and Helen Nissenbaum, Cornell Tech (US) Page 55	Workshop The right of access to police databases organised by Vrije Universiteit Brussel Page 56	Seminar Philosophers' Seminar on Compliance and Automation in Data Protection Law organised by CPDP, ALTEP-DP and COHUBICOL (BE) Page 57
Coffee break			
From Science Fiction to Reality: The Ethics of Body-Technology Interactions organised by IMPAKT (NL), Privacy Salon (B), Werktank (B) and transmediale (D), as part of CODE. Page 53	Novel concepts in digital states and their structures organised by CDSL Page 55	Workshop A GDPR Certification Journey in Practice: How to Prepare for a Europrivacy Audit and the Actual Certificate organised by Timelex Page 57	Seminar Philosophers' Seminar on Compliance and Automation in Data Protection Law organised by CPDP, ALTEP-DP and COHUBICOL (BE) Page 57
Accommodating children's needs online: an impossible task? organised by CLSR Page 54	Working & Meeting Space Page 55	Working & Meeting Space Page 57	Working & Meeting Space Page 57
Closing remarks in Grande Halle	Closing remarks in Grande Halle	Closing remarks in Grande Halle	Closing remarks in Grande Halle
Cocktail sponsored by Privacy Salon in Le Village			

TUESDAY 23RD MAY 2023

18:00 - CPDP2023 OPENING NIGHT - LES HALLES

Co-organised by Brussels Privacy Hub, Nym Technologies, Privacy Salon and Brave

Join us for two immersive conversations on the privacy implications of the "cashless" society and participatory design, followed by a welcome cocktail to officially open the 16th edition of CPDP.

CLOUD MONEY, DATA PRIVACY AND SOVEREIGNTY - WHAT IS AT STAKE AND WHAT CAN BE DONE?

The push to digital payments entails an explosion in the sheer volume of data produced about peoples spending habits, needs and lives. It also entails a radical shift in who controls payment infrastructures, from the public infrastructure of cash, to the private systems of the banking and payments industry. In response central banks are proposing their own digital money in the form of CBDCs. Meanwhile, public is stuck between these trends with little more than a pinky-promise to protect privacy. On this panel of experts, former Central Banker Arauz will speak about the data of money and the relationship between privacy, payments and democracy. Author Brett Scott will describe who wins and who loses from the shift to cashless. And Nym Head of Research Piotrowska will explain some of the cryptographic possibilities, technical risks and remedies when it comes to privacy and payments.

Moderator Jaya Klara Brekke, Nym Technologies (CH)
Speakers Brett Scott, author of Cloud Money (UK/DE); Andres Arauz, former head of Central Bank of Ecuador (EC); Ania Piotrowska, Nym Technologies (CH)

TURNING DATA PROTECTION INSIDE OUT

JULIE COHEN, GEORGETOWN UNIVERSITY (US) - KEYNOTE SPEECH
"FROM SURVEILLANCE VULNERABILITY TO DOUGHNUT PRIVACY"

Followed by a dialogue with

Moderator Gianclaudio Malgieri, Brussels Privacy Hub (BE) and Leiden University (NL)
Speakers Alexandra Geese, MEP Green Party (EU); François Pellegrini, CNIL (FR); Timo Jakobi, Nuremberg University (DE)

In the years since enactment of the GDPR, analysis of data protection and privacy has continued to benefit from new thinking about sustainability, participatory and value-sensitive approaches to design, and explorations of the impacts of digital technologies and data-driven processes on vulnerable populations. After a keynote speech by Professor Julie Cohen about the path from surveillance vulnerability to sustainability in privacy and data protection, the panel will discuss what data protection can learn from discussions about the differential vulnerabilities of data subjects and from new approaches to participatory and value-sensitive design?

COCKTAIL SPONSORED BY BRAVE IN LE VILLAGE [TILL 21.00]

WEDNESDAY 24TH MAY 2023

Please note that this is a preliminary version of the programme.

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

CPDP2023 PANELS AT GRANDE HALLE

08:30 - WELCOME AND INTRODUCTION BY PAUL DE HERT

08:45 – GLOBAL AI GOVERNANCE: POLICY AND PRACTICE

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by International Association of Privacy Professionals (IAPP)
Moderator Caitlin Fennessy, International Association of Privacy Professionals (US)
Speakers Juha Heikkila, DG Connect, European Commission (EU); Denise Wong, Singapore Personal Data Protection Commission (SG); Karine Perset, OECD Working Party on AI Governance (INT); Dennis Hirsch, Ohio State University Moritz College of Law (US)

Countries around the world are advancing AI legislation, guidance and rulemaking. Meanwhile, companies are considering what AI ethics and governance means in practice. Are different jurisdictions approaching this challenge similarly or not? What role will data protection professionals play in building and implementing AI systems within organizations? Join us to discuss areas of alignment and divergence in AI governance and how data protection teams are getting involved.

10:00 - COFFEE BREAK

10:30 – WHAT WILL CHANGE IN 2024?

Academic ☆ **Business** ☆☆ **Policy** ☆☆☆
Organised by Council of Europe (INT)
Moderator Patrick Penninckx, Council of Europe (INT)
Speakers Tamar Kaldani, Council of Europe (INT); Bruno Giancarelli, European Commission (EU); Alex Joel, American University (US); speaker from CGRII/ANPD (BR)

The ratification of the Protocol CETS No 223 amending Convention 108 remains the main priority for the 55 state Parties of Convention 108. And not only, as the European Commission is also advocating at a highest level for its quick entry into force and for that it stays the reference framework for the protection of privacy and personal data in the digital age. This Protocol, adopted in 2018, has already an impact on the level of privacy and the international flow of data, as it contributes to the convergence of privacy regimes around the globe, which will surely intensify once the instrument comes into force. Completing 38 ratifications in 2024, the modernised Convention 108 will, even if partially, enter into force. With this modern(ised) and robust multilateral instrument new possibilities will be opened to elevate the protection of privacy to a global level based on its commonly agreeable and adaptable standards and provisions.

- Will the entry into force of the amending Protocol change anything at all?
- Will the modernised Convention 108 be able to deliver its promises?
- Will individuals be more protected in its state Parties? Globally?
- Will sending data abroad be easier after its entry into force? In the private sector? In the public sector?

11:45 – DOES THE COMPUTER KNOW I AM A CHILD? PROTECTING CHILD RIGHTS IN AN AGE OF ALGORITHMS.

Academic ☆ **Business** ☆☆ **Policy** ☆☆☆
Organised by EU Agency for Fundamental Rights (EU)
Moderator David Reichel, EU Agency for Fundamental Rights (EU)
Speakers Emilia Gomez, European Commission, Joint Research Centre (EU); Leanda Barrington-Leach, International Advocacy 5rights Foundation (INT); Luca Tosoni, Datatilsynet (NO); Cecilia Alvarez, Meta (BE); Carolien Michielsen, Sibbe (BE)

According to the UN Convention on the Rights of the Child and the EU Fundamental Rights Charter children have a right to protection and participation. However, the internet and the use of algorithms have put children's wellbeing at risk: excessive use of online services and exposure to content that is particularly harmful to children raise many questions with respect to safeguarding the rights of the child. As online services are driven by algorithms, measures are needed to prevent algorithms from profiling children online. Secondary EU legislation includes several provisions to support safeguarding fundamental rights of children, including the GDPR, the DSA, and the proposed AI Act, most notably to prohibit profiling of children, e.g. for marketing purposes. However, are these legal requirements enough? How can we make sure that these rules are effectively implemented - notably in a fast-changing digital landscape? Can we even use algorithms to support child protection and participation in the online world?

- What are the main risks to the wellbeing of children posed by social media and other online services considering interplay between protection and participation?
- How does the use of algorithms harm, and how can it help safeguarding child rights online?
- Which provisions in available European law, such as the GDPR and

the DSA, are most promising to increase the protection of children online while at the same time allowing their participation when identified as a child?
- How to make sure that legal provisions are effectively controlled and enforced?

13:00 - LUNCH

14:15 – DIALOGUE ON FRICTION BETWEEN MODERN MARKETING AND ADVERTISING AND GDPR AND EPRIVACY DIRECTIVE: IS THERE AN EFFECTIVE WAY FORWARD?

Academic ☆ **Business** ☆☆☆ **Policy** ☆☆
Organised by Interpublic Group (US)
Moderator Sheila Colclasure, Interpublic Group (US)
Speakers Dale Sunderland, Ireland's Data Protection Commission (IE); Charles Ping, Winterberry Group (UK); Paul Breitbarth, Catawiki (NL); Gabrielle Robitaille, Word Federation of Advertisers (BE)

The Nielsen TV ratings system was born in 1950, facilitating not just knowing how many people watched a program, but also their demographics. The observational nature of the Internet took data driven marketing and advertising to a new and transformative level. The push-back has been data protection analysis that frames all data driven marketing and advertising is asymmetric in its power and manipulative in its effects. There is some truth to this, but persuasive sales also have its place. The push for sellers to find their market and do so efficiently will not disappear. The sense that observation-based selling is "surveillance capitalism" is also a given. Are there ways to reduce the friction between these two tectonic forces in a manner that services the full range of rights and interests? This will be explored as a dialog in this session:

- To examine the challenges that modern marketing and advertising poses to the privacy of individuals and how the GDPR and ePrivacy Directive address these challenges.
- To understand the implications of the GDPR and ePrivacy Directive for businesses that rely on modern marketing and advertising, including the requirement to obtain informed consent from individuals.
- Discuss best practices for businesses that rely on modern marketing and advertising to comply with the GDPR and ePrivacy Directive and how to meet the regulatory requirements without compromising the effectiveness of their advertising campaigns.
- Discuss conflation with other digital practices.
- Provide an opportunity for attendees to ask questions and engage in a dialogue wit the panelists.

15:30 - COFFEE BREAK

16:00 – EXAMINING FUNDAMENTAL RIGHTS IN A NEW ERA OF AI

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by Microsoft (US)
Moderator James Arroyo, Ditchley Foundation (UK)
Speakers Julie Brill, Microsoft (US); Leonardo Cervera-Navas, European Data Protection Supervisor (EU); Karolina Mojzesowicz, Unit Data Protection, European Commission (EU); Deirdre Mulligan, the White House's Office of Science and Technology Policy (OSTP); School of Information at UC Berkeley, Berkeley Center for Law & Technology (US)

Artificial Intelligence may be one of the most transformative technologies that humanity has ever witnessed. The current wave of AI advancement presents both incredible new opportunities in human creativity, understanding and intelligence and potentially new safety, security and privacy consequences if not built responsibly. Today, and in the future, AI will play a central role in our societies and democracies worldwide. To ensure we have safe and secure democratic societies, we cannot afford to halt AI innovation. Just as new types of AI continue to transform our world; questions remain on how we can ensure responsible innovation while protecting our most fundamental human rights.

- What are the implications of this new wave of AI on our collective security and fundamental rights?
- How can we ensure that our current and future global policy frameworks are prepared for the wave of innovation that has just arrived?
- How should future legislation frame the responsibilities of private sector and regulators when it comes to AI governance?
- What can global initiatives on AI governance learn from the ongoing discussions on the AI Act?

17:15 – MOVING TOWARDS A SUSTAINABLE AND FUNCTIONAL EU-US TRANSFERS FRAMEWORK?

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by CPDP
Moderator Christopher Kuner, VUB (BE)
Speakers Thomas Boué, The Software Alliance (BE); Anna Fielder, Transatlantic Consumer Dialogue (EU/US); Bruno Gencarelli, European Commission (EU); Kristina Irion, Institute for Information Law (IViR), University of Amsterdam (NL); Peter Swire, Georgia Institute of Technology, School of Cybersecurity and Privacy (US)

INTRODUCTORY REMARKS BY EUROPEAN COMMISSIONER FOR JUSTICE, DIDIER REYNDERS

For years now, it seems we have been on something of a merry go round regarding transfers between the EU and the U.S. – an adequacy decision is adopted, and then subsequently struck down. Currently, a new EU-US adequacy decision has been proposed and is being discussed: the EU-US Data Privacy Framework. Yet the proposed decision has already been subject to a range of different critiques, from a range of different actors. Against this background, this high-level panel will bring together stakeholders from politics, industry, civil society, and academia, to discuss the status and future of EU-U.S. transfers. Amongst others, the following questions will be discussed:

- What is the status of the EU-U.S. Data Privacy Framework?
- What are the obstacles which remain to its adoption?
- Which criticisms have been put forward against the framework?
- What is the future of the framework moving forward?

18:30 – COCKTAIL SPONSORED BY EDPS

in Le Village

CPDP2023 PANELS AT AREA 42 GRAND

08:30 - WELCOME AND INTRODUCTION BY PAUL DE HERT in Grande Halle

08:45 – EXPLORING THE MANY FACES OF THE GDPR- IN SEARCH OF EFFECTIVE DATA PROTECTION REGULATION

Academic ☆☆☆ **Business** ☆ **Policy** ☆☆
Organised by Haifa Center for Law and Technology, Faculty of Law, University of Haifa (IL)
Moderator Tal Zarsky, University of Haifa (IL)
Speakers Raphaël Gellert, Interdisciplinary Hub for Digitalization and Society, Radboud University (NL); Gabriela Zanfir Fortuna, Future of Privacy Forum (US); Sam Jungyun Choi, Covington & Burling LLP (BE); Amit Ashkenazi, University of Haifa Center for Law and Technology (IL)

The panel aims to contribute to current discussions on the effectiveness of the GDPR by focusing on challenges arising from the regulatory design it sets forth. While the GDPR is obviously a "data protection" law, legal deconstruction reveals that it strives to achieve its objectives by applying and fusing rules and institutions from various legal fields. These include, inter alia, EU law, fundamental rights law, regulatory law, corporate governance and private law. These measures, in turn, focus their attention on the behavior of individuals, enforcement agencies and corporations. Reflecting on the breadth of these measures provides new insights as to the challenges of deploying the GDPR. In addition, although these measures share a common goal, they might be in tension if not conflict, with each other due to their different legal nature, thus generating inefficiency. The discussion of these issues is crucial for properly establishing priorities in GDPR application, as has relevance to other developing multifaceted regulatory areas, such as Artificial Intelligence.

- How have different legal fields and enforcement measures inspired the GDPR, and the roles for DPAs, companies and data subjects?
- The GDPR aims to protect the fundamental rights of individuals through various measures – how has it been faring?
- What can we learn from developments in regulation theory and corporate governance so to promote more effective data protection "accountability"?
- How can these lessons learned from other regulatory settings be applied to developing data protection frameworks in other jurisdictions?

10:00 - COFFEE BREAK

10:30 – REFORMING THE ADTECH ECOSYSTEM: OPTIONS FOR CHANGE BEYOND THE E-PRIVACY DIRECTIVE, DSA AND DMA

Academic ☆☆☆ **Business** ☆ **Policy** ☆☆
Organised by AWO Agency
Moderator Nick Botton, AWO Agency (UK)
Speakers Johnny Ryan, Irish Council for Civil Liberties (IE); Angela Mills Wade, European Publishers Council (EU); Peter Eberl, European Commission (EU); Alexandra Geese, European Parliament (EU)

A new EU study conducted by AWO found that the digital advertising market is unsustainable: on the one hand, fundamental rights are undermined by the market's focus on personal data, profiling and tracking, and on the other, publishers and advertisers complain about their lack of control and lack of competition. Indeed, the market is beset by a variety of problems: lack of transparency, lack of user control over their personal data, high energy intensity, fraud, dependency on large platforms, and ads funding harmful content, among others. Legislation such as the GDPR, ePrivacy Directive, DMA, DSA, and consumer protection law does not address all of these problems, and the market's rapid evolution and complexity act as clear barriers to effective enforcement. This panel will combine expertise from the policy, industry and digital rights sector to discuss the gaps in EU law applicable to the digital advertising market. Its aim will be to help chart the way forward for future EU legislation to make the digital advertising market more balanced and sustainable.

- Beyond the DMA, how can the digital advertising market be made more balanced and transparent?
- Beyond the GDPR, ePrivacy Directive and consumer law, how can we increase user control over their personal data in digital advertising?
- Beyond the DSA's bans on targeting to minors and based on sensitive data, should other practices in the market be forbidden?
- How can the market be improved from an advertiser and publisher perspective while at the same time protecting fundamental rights?
- How can we encourage the growth of alternative models of digital advertising that rely on less personal data?

11:45 – A MARKET OF ONE: PERSONALISED PRICING FROM A DATA, COMPETITION AND CONSUMER PROTECTION PERSPECTIVE

Academic ☆☆☆ **Business** ☆ **Policy** ☆☆
Organised by The European Consumer Organisation (BEUC)
Moderator Ursula Pachl, The European Consumer Organisation (BEUC) (BE)
Speakers Gaetano Lapenta, OECD (INT); Harmonie Vo Viet Anh, Eyeo (DE); Petra Leupold, VKI Academy (AT); Aymeric Pontivianne, CNIL (FR)

"Consumers want personalised offers and experiences". "Personalisation ensures customers receive the best deal they can get". These quotes could be easily attributed to a tech company executive. The technological means to personalise prices online are extensive and developing rapidly. Companies use profiling and data analytics to tailor prices and offers to the extent that an individual becomes a market in oneself. With first grade price personalisation, consumers cannot compare prices any longer and a reference price for the market does not exist anymore. The aim is often to extract the maximum that an individual is willing to pay, or to vary prices to reflect the cost of serving individual customers. How can we have fair and transparent markets in this situation? Do competition, consumer and data protection regulate price personalisation adequately and protect consumers from abuse?

- What are the harmful effects that personalised pricing has for consumers?
- What are the legal issues that personalised pricing raises from a competition, consumer and data protection law perspective?
- How should regulation address personalised pricing to adequately protect consumers?
- How can we tackle unfair personalised pricing practices through the interdisciplinary enforcement of competition, data protection and consumer law?

13:00 - LUNCH

13:00 – CHAT CONTROL: LURKING SURVEILLANCE STATE?

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by Privacy Platform (BE)
Speakers Arda Gerkens, Expertisebureau Online Kindermisbruik (NL); Ella Jakubowska, European Digital Rights (EDRi) (EU); Moritz Körner, Member of European Parliament (EU); Helena Charles, WhatsApp (BE)

The proposal for a regulation to prevent and combat child sexual abuse online is subject of huge controversy. If it is up to the Commission, our private chats will be no longer confidential, and scanned for potential child sexual abuse material and grooming. By essentially putting encryption in the bin, the EU risks creating a mass surveillance system. This panel brings together speakers from civil society, big tech and child safety organisations together to find solutions for tackling child sexual abuse online without infringing upon children's and adults' privacy and creating a mass surveillance system.

- Why is the chat control proposal problematic?
- What are its broader implications?
- How can child sexual abuse online be tackled in a different way, with less privacy infringement?

14:15 – MODEL CLAUSES GO GLOBAL: EU-ASEAN COOPERATION

Organised by European Commission (EU)
Moderator Gabriela Zanfir-Fortuna, Future of Privacy Forum (US)
Speakers Denise Wong, Deputy Commissioner of the Personal Data Protection Commission of Singapore (SG); Alisa Vekeman, International Affairs and Data Flows, European Commission (EU)

Model clauses are an instrument that is increasingly used for data transfers in different systems around the world. Two systems that have developed such clauses are the European Union (Standard Contractual Clauses) and the Association of Southeast Asian Nations (Model Contractual Clauses). Since both clauses share a number of commonalities, the EU and ASEAN are working together to further facilitate their use. This notably includes the publication of a Guide to assist companies present in both jurisdictions with their compliance efforts under both sets of clauses. This panel will explore the role and benefits of model clauses as a transfer instrument and the objective of this new dimension of the cooperation between the EU and ASEAN.

- What has led the EU and ASEAN to adopt or modernise model data protection clauses for data transfers?
- What are the benefits of such model clauses (for businesses, individuals, etc.?)
- What is the purpose of the Guide and what next steps are foreseen?
- What are the opportunities for further cooperation between the EU and ASEAN in this area?
- Are there opportunities for cooperation on model clauses beyond the EU-ASEAN dimension?

15:30 - COFFEE BREAK

16:00 – FROM NOTORIOUS RULE BREAKER TO PRIVACY ADVOCATE: HOW GOVERNMENT CAN CHANGE ITS STRIPES

Academic ☆ **Business** ☆ **Policy** ☆☆☆☆
Organised by Bits of Freedom (NL)
Moderator Evelyn Austin, Bits of Freedom (NL)
Speakers Cecile Schut, Autoriteit Persoonsgegevens (NL); Sjoera Nas, Privacy Company (NL); Estelle Massé, Access Now (BE); Ron Roozendaal, Ministry of Internal Affairs (NL)

This panel will explore the coherence between the work of all stakeholders involved in protecting people's privacy. From drafting laws and regulations, complying with privacy law and enforcing it, to challenging the rules and the rule-breakers: although all stakeholders act autonomously, their work is deeply intertwined. This is a panel of diverse experts: each one of them has a specific role in this system. And each brings years of experience, some even in multiple capacities. That's a perfect basis for shared reflection on the state of play. Initial questions we'd like to explore are:

- Assuming we have the common goal of protecting people's privacy, where and why does the system (in some cases) fail to do so?
- What can we learn from individual experiences?
- What do each of us need to excel in our role?
- How can we best align our efforts?

17:15 – LOOKING BEYOND THE EU DATA STRATEGY: WHERE NEXT FOR DATA USE AND REGULATION?

Academic ☆ **Business** ☆☆ **Policy** ☆☆☆
Organised by Ada Lovelace Institute (UK)
Moderator Valentina Pavel, Ada Lovelace Institute (UK)
Speakers Adriana Nugter, Independent consultant and author of Transborder Flow of Personal Data within the EC (NL); Katarzyna Szymielewicz, Panoptykon Foundation (PL); Inge Graef, Tilburg University (NL); Theresa Stadler, École Polytechnique Fédérale de Lausanne (EPFL) (CH)

Despite the new EU digital package of regulation nearly completely adopted, many fundamental questions still remain open. Current regulation does not go far enough in terms of challenging the dominant business model based on data exploitation. At the same time, large companies gain more and more power from drawing inferences about people, deriving insights based on information that might be about you. This deepens power and information asymmetries, brings novel risks from inference predictions, and opens questions whether we might need a paradigm shift to data regulation.

Central to the Ada Lovelace Institute's work to 'rethink data' is the question: 'What is a more ambitious vision for data use and regulation that can deliver a positive shift in the digital ecosystem towards people and society?' This is explored in the report publication on Rethinking data and rebalancing digital power, looking at four areas of change across infrastructure, governance, institutions and public participation.

The aim of this panel is to reflect critically on fundamental questions that are left unaddressed by existing regulation and use of data, as well as on potential opportunities that can prepare the ground for more ambitious transformations in data-driven systems that benefit people and society.

- What are some of the fundamental questions we need to tackle, beyond the EU Data Strategy?
- How can we challenge the wider socio-technical and economic infrastructures that enable the vast collection, management, and sharing of data?
- At the confluence between data and AI, do we need a new paradigm for how we understand data processing and identification in light of inferential analytics?
- How is the economy of incentives changing in digital markets with the adoption of the new EU regulatory package?

18:30 – COCKTAIL SPONSORED BY EDPS

in Le Village

CPDP2023 PANELS AT AREA 42 MIDI

08:30 - WELCOME AND INTRODUCTION BY PAUL DE HERT in Grande Halle

08:45 – MEASURING DARK PATTERNS AND THEIR HARMS: A MULTIDISCIPLINARY, ANTICIPATORY PERSPECTIVE

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg (LU)
Moderator Marie Potel, Amurabi (FR)
Speakers Felix Mikolasch, NOYB (AU); Arianna Rossi, SnT University of Luxembourg (LU); Cristiana Santos, Utrecht University (NL); Caroline Sinders, ICO (UK)

Dark patterns are under the spotlight in policymaking, research and practice: the DSA, DMA, AI Act and Data Act proposals define them as design elements that impair user autonomy and informed decisions. However, the impact on autonomy is difficult to prove, whereas focusing only on graphical interface elements might not account for next-generation deceptive patterns that emerge from personalised hypernudges, human-robot manipulation, voice and haptic interfaces, etc. But how might we reliably detect, test, measure and regulate digital influences when they are so varied and since identifying what constitutes manipulation is often based on more or less paternalistic views? The individual and collective perception of adverse effects, as well as demonstrable direct and indirect harms, may be ideal proxies to identify and report dark patterns.

- Which attributes can we leverage to reliably measure the presence of dark patterns in digital services?
- Which legal, technical and design instruments do we need to quantify dark patterns' harms at large?
- How might we determine the risks engendered by dark patterns and are these more severe for certain "vulnerable" users?
- How might we detect manipulation and potential for harm in emerging technologies?

10:00 - COFFEE BREAK

10:30 – DATA PROTECTION AUTHORITIES IN EMERGENCIES

Academic ☆☆☆ **Business** ☆ **Policy** ☆☆
Organised by CPDP
Moderator Ivan Szekely, Central European University (HU)
Speakers Charles Raab, University of Edinburgh and The Alan Turing Institute (UK), Pille Lehis, Estonian Data Protection Inspectorate (EE); Chloé Berthélémy, EDRi (BE); Zoe Kardasiadou, DG Just (EU)

Data protection authorities (DPAs) are responsible for protecting the privacy of personal data, but states of emergency and exceptional circumstances often require that laws and rules be set aside or interpreted in ways that override data protection in favour of implementing competing values and rights. This may often occur where 'big data' sources, algorithms, artificial intelligence, and surveillance instruments are used for identifying and tracking people or in disaster relief. Some would argue that emergencies should not suspend or weaken the protection of privacy and personal data provided by DPAs in exercising their roles. However, others would argue that wartime, terrorism, natural or human-made disasters such as earthquakes and tsunamis, mass displacement of people and international migration, and providing humanitarian relief are occasions that challenge data protection on ethical, human-rights, and practical grounds. Panellists will report on the experience of DPAs, emergency-relief and human rights organisations, and give views on these dilemmas, exploring the issues and ways in which they may be resolved.

- What experience and problems have DPAs had in protecting or overriding privacy in emergency situations?
- What experience and problems have emergency-relief and human rights organisations had in protecting or overriding privacy in emergency situations?
- How have DPAs tried to reconcile or 'balance' the competing demands?
- Have DPAs discussed these dilemmas with each other and with emergency-relief organisations informally or in formal meetings across countries or jurisdictions?

11:45 – ADDRESSING THE DIGITAL DIVIDE TO ACHIEVE EQUAL AND INCLUSIVE HEALTHCARE IN EUROPE

Academic ☆☆☆ **Business** ☆ **Policy** ☆☆
Organised by Tilburg Institute for Law, Technology, and Society (TILT) (NL)
Moderator Taner Kuru, TILT (NL)
Speakers Nisha Shah, University of Oxford (UK); Robin van Kessel, Maastricht University (NL); Mindy Nunez Duffourc, Penn State Dickson Law (US); Anna Odone, European Public Health Association/ University of Pavia (IT); Owe Langfeldt, DG SANTE (EU)

Emerging digital health technologies are considered to have the potential to transform healthcare and make it more accessible for everyone. However, while various stakeholders are processing more and more health and genetic data towards this promise, the existing digital divide within Europe might potentially prevent this transformation from achieving its full potential. If left unaddressed, existing inequalities in accessing both healthcare and digital services in Europe might lead this digital transformation to exacerbate the existing disadvantages that vulnerable populations have in accessing healthcare services since they will be unable to benefit from these developments due to, among others, lack of representative data, difficulties in accessing relevant services or technologies, underdeveloped digital literacy skills. This panel will explore the potentials and pitfalls of the existing and upcoming European Union legislation to address these challenges and their implications in practice.

- What are the main reasons for existing inequalities in accessing healthcare in Europe?
- How can the ongoing digital transformation in healthcare exacerbate the disadvantages of vulnerable groups in accessing these services?
- How should the existing digital divide be addressed to achieve equal and inclusive healthcare in Europe through digital transformation?
- Whether and to what extent can we address and tackle this digital divide through legislation?

13:00 - LUNCH

14:15 – VULNERABLE WHO? VULNERABLE WHEN? VULNERABLE TO WHAT?

Academic ☆☆☆ **Business** ☆ **Policy** ☆☆
Organised by VULNERA - the International Observatory (BE)
Moderator Mireille Hildebrandt, Vrije Universiteit Brussel (BE)
Speakers Simone van der Hof, Leiden University (NL); Fanny Coudert, European Data Protection Supervisor (EU); Gianclaudio Malgieri, Leiden University (NL); Mariana Marques Rielli, Data Privacy Brasil Research Association (BR); Malavika Raghavan, London School of Economics (UK)

When understanding how data protection and privacy law puts safeguards in place to protect human vulnerability, it is crucial to start with understanding who are the vulnerable people and groups that need protection, in which contexts and to what harms. This panel will discuss how to define vulnerability in a relevant way for the data-driven society before exploring the actual mechanisms in data protection law and in the broader European Digital Strategy (mostly the DSA and the AIA) to ensure the protection of vulnerable and marginalised people.

- What is the best way to address vulnerabilities of data subjects, users, citizens?
- Is the definition of vulnerable people in the AIA adequate?
- Is the DSA a relevant addition to protect human vulnerabilities online?
- Are there active participative models that could mitigate marginalisation, power imbalance and vulnerability?

15:30 - COFFEE BREAK

16:00 – DUTIES OF DATA LOYALTY AND THE FUTURE OF DATA PROTECTION

Academic ☆☆☆ **Business** ☆ **Policy** ☆☆
Organised by Cordell Institute, Washington University in St. Louis (US)
Moderator Neil Richards, Cordell Institute at Washington University in St. Louis (UK)
Speakers David Erdos, University of Cambridge (UK); Carolina Foglia, European Data Protection Board (IT); Woodrow Hartzog, Boston University, (US); Claudia Haupt, Northeastern University (DE); Orla Lynskey, London School of Economics (IE)

Lawmakers in Europe and the United States have enacted or are considering duties of data loyalty as a way to supplement or anchor data privacy regimes. For example, the Data Governance Act contemplates loyalty obligations on intermediaries as part of a fiduciary obligation; California and the United Kingdom's Age Appropriate Design Codes prioritize the "best interests" of children in the design of digital technologies; and the proposed American Data Protection and Privacy Act is anchored by a duty of loyalty requiring robust data minimization and specific loyal data practices. This panel will consider these efforts, their effectiveness, their limits, and their possible future as a complement to established data protection rules. It will address how loyalty is conceptualized and clarified, how loyalty duties are balanced with other obligations, and how they might differ in the E.U. from the United States.

- How should data loyalty be conceptualized?
- What should specific loyalty rules look like?
- How should duties of data loyalty deal with competing values and co-existing loyalty obligations?
- How should data loyalty be situated within larger privacy and data protection frameworks?

17:15 – FROM THEORY TO PRACTICE: DIGITAL CONSTITUTIONALISM AND (DATA) JUSTICE ACROSS THE GLOBE

Academic ☆☆☆ **Business** ☆ **Policy** ☆☆
Organised by Data Privacy Brasil Research Association/DPBR (BR)
Moderator Mariana Marques Rielli, Data Privacy Brasil Research Association (BR)
Speakers Laura Schertel Mendes, University of Brasília (BR); Linda Bonyo, Lawyers Hub Africa (KE); Katerina Demetzou, Future of Privacy Forum (BE)

While an exponential number of comprehensive data protection laws are currently in place across the globe, with a rapid expansion in Global South countries, it is important to note that specific social, political and legal contexts also translate into different values and priorities, and that the path towards what would constitute meaningful privacy/ data protection can vary. On the one hand, a vibrant field of comparative study of data protection regimes around the world has been emerging, not least in the drive for regulatory convergence - particularities must be carefully understood for common solutions to arise. At the same time, and perhaps more interesting, are the examples found in other, broader, strategies to not only deal with eventual data processing implications on individual data subject's rights, but rather the wide implications of datafication processes over individuals, collectives, public-private relationships, political regimes, etc. Throughout the extremely diverse countries and regions that make up the so-called Global South, histories of political and social struggles have given rise to legal strategies to counter violations of privacy and data protection by way of defending other fundamental rights, such as due process and civil rights, in general. More recently, strategic litigation to counter surveillance and privacy harming practices has leaned on constitutional provisions (both data protection and otherwise) where data protection legal regimes may not be fully applicable. The panel will seek to explore the underlying questions around constitutionalization of data rights and what that entails for meaningful data protection and strategic litigation. Some of the questions that will be discussed are:

- What are the gains, in practice, of inscribing data protection in constitutional provisions when it comes to enforcing rights?
- Considering in some legal regimes data protection is a corollary of other fundamental rights and values, how can strategic litigation at the constitutional level be effective?
- Are the concepts of datafication and data justice useful to describe and address how information capitalism is reshaping and reinforcing the asymmetry of power in the relationships between citizens, governments and corporations? How does that play, if at all, into legal debates?
- What lessons can be derived from the experiences of strategic litigation to protect privacy and data protection (in all countries/regions represented in the panel)?

18:30 – COCKTAIL SPONSORED BY EDPS

in Le Village

WEDNESDAY 24 MAY 2023

CPDP2023 PANELS AT LA CAVE

08:30 - WELCOME AND INTRODUCTION BY PAUL DE HERT in Grande Halle

08:45 – YOUTH PRIVACY PROTECTION AND ONLINE GAMING

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by Université de Paris-Saclay and INSA Centre Val de Loire (FR)
Moderator Benjamin Nguyen, INSA Centre Val de Loire (FR)
Speakers Nicoletta Corrocher, Universita' Bocconi (IT); Pierre-Luc Déziel, Université Laval (CA); Marie Duboys-Fresney, CNIL (FR); Jürgen Bänsch, Interactive Software Federation of Europe (BE)

94% of under 18 minors play computer games. 60% of them play online and 52% of them play every day. When compared to the general population, where only 37% play every day, most minors (64%) feel that signing onto an online game is a common action, and that they should be allowed to do it unsupervised from 14 years old. In other words, mass consumption of online gaming by minors is the norm today. However, such use by a very young public asks many questions concerning privacy protection: indeed, in principle parental consent is needed, but in reality, this is greatly ignored. The objective of this panel is to discuss the legal, economic, technical and regulation aspects to offer a better protection to under 18 minors, while preserving innovation of the gaming industry.

- What is specific to data processed and published in online games?
- What are the risks of misuse of internal and published data concerning minors in online games?
- What proposals to improve data protection of under 18 minors in online games?
- How should the gaming industry be assisted to achieve these goals?

10:00 - COFFEE BREAK

10:30 – CHRONICLE OF A DEATH FORETOLD: IS EU PREDICTIVE SECURITY POLICY KILLING DATA PROTECTION?

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by Free Group (EU)
Moderator Emilio De Capitani, Free Group (EU)
Speakers Birgit Sippel, Member of European Parliament, LIBE Committee (EU); Anze Erbeznik, European Parliament/European Law Faculty (SI); Merve Hickok, Centre for AI and Digital Policy (US); Catherine Forget, Ligue of droits de l'homme (FR); Douwe Korff, EU and CoE expert on data protection (EU);

Paradoxically, it has been after Lisbon and the establishment of a specific legal basis in EU Treaties that data protection has been progressively dismantled by a combined action of the Commission and Interior Ministers in the Council. The European Parliament gave up. And only Data Protection Authorities and the Court of justice are still standing but with several difficulties as EU institutions do not comply with rulings on data protection (EU-US privacy Shield, PNR Directive, Data Retention). Moreover, in the JHA several instruments are being adopted based on a new private-government cooperation blurring the line between GDPR and LED, data controller and data processor, and territoriality (e-evidence). Further, intrusive instruments based on a "false" legal basis of Art. 114 are being adopted challenging classical law enforcement and data protection understanding (e-privacy derogation). The EU is following the preventive security model.

- Is the EU following the US and soon the Chinese model of Predictive policy?
- How such a trend can be reversed?
- How the tricky "consistency mechanism" of the Data Protection legal framework and the lack of a stronger role of the EDPB is de facto paving the way to dismantle Data Protection?
- How the European Parliament is cornered by the Council and the Commission and is losing its role of defending a true supranational freedom, security and justice area?

11:45 – AI ACT FOR ALL PEOPLE? INTERROGATING EUROPE'S AI REGULATION FROM THE MIGRATION PERSPECTIVE

Academic ☆☆ **Business** ☆ **Policy** ☆☆
Organised by European Digital Rights (EDRi) (BE)
Moderator Sarah Chander, EDRi (BE)
Speakers Caterina Rodelli, Access Now (INT); Alyna Smith, Platform for International Cooperation on Undocumented Migrants (PICUM) (BE); Anna Moscibroda, DG JUST, European Commission (BE); Niovi Vavoula, Queen Mary University of London (UK)

As the European Union amends the Artificial Intelligence Act (AI Act) exploring the impact of AI systems on marginalised communities is vital. AI systems are increasingly developed, tested and deployed to judge and control migrants and people on the move in harmful ways. This panel explores the various ways AI systems fit within a broader context of surveillance, criminalisation and punishment of migrants and people on the move. Tracking EU level political developments, including in the European Parliament, Council and perspectives from civil society, the panel asks, how can AI regulation prevent harm and ensure protection for all people, regardless of migration status?

- How are AI systems developed and used in ways that impact people on the move?
- How did the EU's AI act initially address this?
- What is the status of the political deliberations, and what have civil society been doing to influence this?
- What needs to happen to prevent AI-based harms against people on the move?

13:00 - LUNCH

14:15 – NON-COMPULSORY GOVERNMENT ACCESS TO DATA: THE NEXT FRONTIER FOR SURVEILLANCE REFORM?

Academic ☆ **Business** ☆ **Policy** ☆☆☆☆
Organised by Stiftung Neue Verantwortung e.V. (DE)
Moderator Thorsten Wetzling, Stiftung Neue Verantwortung (DE)
Speakers Julia Thorsøe Ballaschk, National Special Crime Unit (SCU), Danish Police (DK); Judith Lichtenberg, Dutch Intelligence Oversight Body CTIVD (NL); Tomaso Falchetta, Privacy International (UK); Paula Cipierre, Palantir Technologies (DE)

Law enforcement agencies and intelligence services across Europe are increasingly processing a wide array of 'commercially available data' and a broad range of information they deem 'publicly available'. The private sector entities which provide or facilitate government access to such data are often not obliged by law to do so. Unlike many modes of compelled and direct government access to data, governments' various non-compelled acquisitions and subsequent processing of commercially and publicly available data face fewer legal restrictions and authorisation requirements and less oversight. This panel convenes experts and practitioners to shed different lights on these newer modes of public-private co-productions of surveillance. What is their relevance and what challenges arise as regards their regulation, the protection of fundamental rights and freedoms and their democratic governance?

- Has the quantity and quality of commercially and publicly available data transformed the practice of policing and intelligence as we know it?
- What room, if any, should democracies leave for voluntary or non-compelled government access to data?
- What challenges arise as regards their regulation, the protection of fundamental rights and freedoms and their democratic governance?
- How can disproportionate LEA/SIS use of commercially and publicly available data best be prevented?
- What more can be done at the regional level to help insulate democracies from illiberal practice without abandoning key tools for their security?

15:30 - COFFEE BREAK

16:00 – INTEROPERABILITY IN THE EU'S AFSJ: PREPARING TO SUPERVISE THE "POINT OF NO RETURN"

Academic ☆☆☆ **Policy** ☆☆☆
Organised by European Data Protection Supervisor (EDPS) (EU)
Moderator Fanny Coudert, European Data Protection Supervisor (EDPS) (EU)
Speakers Niovi Vavoula, Queen Mary, University of London (UK); Clara Guerra, Portuguese Data Protection Authority (PT); Justine Piret, Directorate-General Migration & Home Affairs, Digital Schengen Unit, European Commission (EU); Ann-Charlotte Nygård, Fundamental Rights Agency (EU)

With the implementation of the interoperability architecture foreseen by 2024, the linking of EU border management and criminal databases will lead to the large scale processing of personal data of almost every third country national travelling to, moving within, and exiting the EU (and for years after). In 2018, the EDPS stated that the decision of the EU legislator to make large-scale IT systems interoperable would 'not only permanently and profoundly affect their structure and their way of operating, but would also change the way legal principles have been interpreted in this area so far and would as such mark a "point of no return."' With that point now approaching, the sheer volume and complexity of the data flows foreseen, multiplicity of controllers, and facilitation of law enforcement access are confronting supervisory authorities with significant challenges, and require thorough consideration.

- How to uphold principles of transparency and fairness, and ensure data subject rights?
- How to supervise an ecosystem of processing operations across multiple controllers?
- How to audit algorithmic profiling (embedded in ETIAS and VIS) to ensure it is targeted, proportionate and non-discriminatory?
- What does interoperability mean concretely for individuals: its impact on fundamental rights, on human agency, autonomy and human dignity; as well as on certain categories of individuals, and for our societies?

17:15 – SHINE A LIGHT: DATA PROTECTION AND LAW ENFORCEMENT IN THE DIGITAL AGE

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by Europol Data Protection Experts Network (EDEN) (EU)
Moderator Els de Busser, Institute of Security and Global Affairs, Leiden University (NL)
Speakers Floor Jansen, Dutch Police (NL); Helen Gibson, Sheffield Hallam University (UK); Pete Fussey, University of Essex (UK); Jürgen Ebner, Europol (NL)

This panel on data protection in law enforcement will cover an operational use case by the Dutch police linked to Darknet investigations and from there move on to a broader debate regarding the data protection accountability principle in various contexts including the use of artificial intelligence. It will address public concerns of mass surveillance by demystifying law enforcement processing operations upon personal data and shed light on what the actual challenges are.

- What are the key challenges for law enforcement when it comes to the use of encryption and anonymisation technologies that conceal the identity of users and the data they exchange?
- How can artificial intelligence be used by law enforcement in a responsible manner?
- What lessons can be drawn from a data protection perspective comparing policing in the UK and the EU following the Brexit?
- Which challenges does Europol face when implementing its applicable data protection legal framework in practice?

18:30 – COCKTAIL SPONSORED BY EDPS

in Le Village

WEDNESDAY 24 MAY 2023

CPDP2023 PANELS AT AREA 42 PETITE

08:30 - WELCOME AND INTRODUCTION BY PAUL DE HERT in Grande Halle

08:45 – HOW TO DETERMINE THE RIGHT ANONYMISATION MEASURES IF THE TERM "PERSONAL DATA" IS UNCLEAR? FINDING THE MISSING PIECES FOR A FUNCTIONAL ANONYMISATION FRAMEWORK

Academic ☆☆☆ **Business** ☆☆ **Policy** ☆
Organised by Einstein Center Digital Future / Berlin University of the Arts (DE)
Moderator Karolina Mojzesowicz, Unit Data Protection at European Commission (EU)
Speakers Valentin Rupp, Einstein Center Digital Future / Berlin University of the Arts (DE); Mark Elliot, University of Manchester (UK); Andrea Gadotti, Imperial College London (UK); Maryline Laurent, Télécom SudParis (FR

The correct specification of the GDPRs scope continues to pose a difficult quest for stakeholders in a data-driven society. Anonymisation approaches, such as k-anonymity or differential privacy, are supposed to offer a way for safe and legally sound data processing. However, as long as the concept of personal data is not sufficiently clarified, it is impossible to reliably answer the question of the right anonymisation measure (not to mention the right k or ε) - at least not from a legal perspective. This panel tries to reconnect the question of anonymisation with what it was supposed to protect all along: personal data and thus the fundamental rights of the data subjects (see Art. 1 sect. 2 GDPR). Can a closer look on the fundamental rights offer a scale that is even able to determine the required k and ε?

- What is the current state of anonymisation in practice?
- Using a sledgehammer to crack a nut - are anonymisation techniques being used ineffectively?
- How can anonymisation be improved in terms of legal certainty?
- What is the view of data protection authorities on this?

10:00 - COFFEE BREAK

10:30 – BLOCKCHAIN-BASED IDENTITY MANAGEMENT SYSTEMS: OPPORTUNITIES AND CHALLENGES

Academic ☆☆☆ **Business** ☆☆ **Policy** ☆
Organised by Centre for IT & IP Law, CiTiP, KU Leuven (BE)
Moderator Jessica Schroers, CiTiP, KU Leuven (BE)
Speakers Alexandra Giannopoulou, University of Amsterdam (NL); Bilgesu Sumer CiTiP, KU Leuven (BE); Paolo Campegiani, Project Leader for ISO-decentralized identifiers (IT); Simaran Jindal, IBM (SW)

In recent years, blockchain technology has triggered public and legal debates among others, regarding its tension with the GDPR. For instance, the GDPR is predicated on the idea that in each data processing activity, there is always at least one natural or legal person ("data controller") who is accountable for compliance and can be requested to fulfill the rights of data subjects. However, the polycentric nature of blockchains seems to challenge this logic. Furthermore, it is practically impossible to delete the data on the blocks, which further endangers the applicability of the right to be forgotten. At the same time, the European Digital Identity Regulation proposal amending the eIDAS Regulation, is opening the way for new regulatory technical measurements, including tamper-proof electronic ledgers. It also includes references to self-sovereign identification, timestamps, and data integrity, giving stakeholders evidence of identity verification.

Consequently, stakeholders are confronted with several legal issues in developing blockchain-based identity management systems, including trust service providers defined in the eIDAS and the proposal.

This panel will focus on the interplay between the GDPR and the proposed eIDAS 2.0; state-of-the-art blockchain-based identity management systems, including Self-Sovereign Identity and biometric recognition. The aim is to provide a brief overview of the applications' main components, taking into account the opportunities and challenges for data protection. The panel will discuss, among others, the following:

- What is the rationale for the use of blockchain-based identity management systems?
- How do such infrastructures operate?
- What are the benefits and risks of such systems?
- What are the legal challenges for fundamental rights and freedoms and data protection, particularly when biometric data are integrated into these systems?
- What could be the safeguards against the discussed risks?

11:45 – HOW TO MAKE PRIVACY MORE USER-FRIENDLY FOR THE LONG-TERM

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by EPFL Center for Digital Trust (CH) and UC Berkeley Center for Long-Term Cybersecurity (US)
Moderator Robin Wilton, Internet Society (UK)
Speakers Hanlin Li, UC Berkeley Center for Long-Term Cybersecurity (US); Jhalak Kakkar, National Law University Delhi (IN); Paul Nemitz, European Commission (EU); Carmela Troncoso, EPFL Security and Privacy Engineering Lab (CH)

Already today privacy, data security and transparency are at peril. Legal frameworks vary globally creating loopholes and compliance dilemmas for companies whilst leaving consumers vulnerable and confused as they click through cookie consents and privacy notices. Behind the scenes, the data collected feeds into algorithms that amplify disinformation, hate speech and discrimination, and is sold to data brokers for use in profiling and micro-targeting. Meanwhile too little data is available for research in the public interest. Now, imagine these challenges on steroids by 2030 as new technologies and actors emerge. How can technological and policy innovation strengthen privacy and protect users more effectively?

This discussion at the intersection of people, policy and technology will engage participants in long-term thinking to help make privacy lastingly more user-friendly, and explore how latest technology progress and new governance models can help to achieve this goal.

- Looking beyond our preoccupations today, what trends and critical uncertainties that will reshape privacy and digital trust by the end of this decade are currently overlooked?
- From data minimization to stronger liability clauses, what are policy and regulatory solutions to current and future challenges that will close loopholes for companies, increase efficiency and put the users and communities at the center?
- From end-to-end encryption to decentralization, what new, concrete practical and technological solutions are emerging that make privacy more usable and user-friendly? Or that might make security and privacy even "invisible" to the user as they will be embedded in systems and architectures from the get-go?
- To strengthen digital trust over the next decade, what concerns need to be considered and what investments need to be made, to ensure global equity while avoiding a patchwork in which privacy becomes a luxury good for some?

13:00 - LUNCH

14:15 – THE EHDS AND SECONDARY USE OF DATA: IS IT POSSIBLE TO BALANCE INDIVIDUAL INTERESTS WITH THE ULTIMATE NEED FOR DATA SHARING TO FACILITATE RESEARCH?

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by Vrije Universiteit Brussel, Health and Ageing Law Lab (LSTS, HALL) (BE)
Moderator Paul Quinn, VUB (LSTS, HALL) (BE)
Speakers Pauline Granger, Sanofi (FR); Sara Roda, Committee of European Doctors (EU); Anastasiya Kiseleva, VUB (HALL, LSTS) (BE), CYU (ETIS) (FR); Nerea Peris Brines, EDPB (BE)

The proposed European Health Data Space represents a radical idea that is likely to fundamentally change the way health data is used and shared across Europe. Its proposals to facilitate the increase secondary use of health data for scientific research will bring about an increased level of data sharing and seemingly reduce the importance of obtaining consent in many forms of research. Whilst it is hoped that the EHDS will go some way to redressing a perceived research gap that has opened up between Europe and the US, significant concerns exist surrounding the protecting of individual interests, especially in terms of privacy and data protection. This panel will explore some of these issues, looking at both the promises and the challenges the EHDS brings with it.

- The secondary use of health data: is it the revolution in legal regimes for data?
- How may the secondary use of health data facilitate the scientific research?
- Is the secondary use of health data compatible with data protection, privacy, and other interests of individuals?
- The EHDS and secondary use of health data: what is the direction to move forward?

15:30 - COFFEE BREAK

16:00 – DIGNITY, TECHNOLOGY AND HUMAN VALUES IN SMART TECHNOLOGICAL ENVIRONMENTS: FROM DESIGN TO THE LIVED EXPERIENCE

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by Centre for Research into Information, Surveillance and Privacy (CRISP) (UK)
Moderator William Webster, CRISP (UK)
Speakers Philippa Hedley-Takhar, Design for Dignity (UK); Hielke Hijmans, Belgian Data Protection Authority (BE); Anaj Puri, Tilburg University (NL); Carolyn Wilson-Nash, University of Stirling (UK)

An established line of thinking promotes the importance of designing human values into the development of technology. Values include dignity, fairness, autonomy, and transparency, and go beyond fundamental legally recognised human rights. The dominant view is that these values will not naturally be accommodated and there must be a conscious effort to design technology to facilitate these values. The emergence of smart technologies, such as AI, with their opaque information processes, has proven to be challenging. There is a clear movement to ensure appropriate governance and oversight of their use, in order to fuel the promotion of human values and at the same time manage potential risks. The GDPR and the proposed AI Act illustrate the growing importance of designing-in the regulation of AI and other data-processing systems, and the human values in question have been among those articulated in the host of ethical frameworks produced in recent years. This panel explores the process of designing-in human values by contrasting the design phase of development with the lived experiences of those using the technology. The panel highlights discrepancies in design and implementation, as well as valuable lessons about how to enhance the design process.

- What are human values and what is the relationship between human values and new technology?
- How can human values be designed into new digital technology, including AI?
- Are there any lived experience examples of how digital technologies reflect previous attempts at designing in human values?
- How can the process of technology design be enhanced by lived experiences to better reflect the importance of human values?

17:15 – WHO IS VISIBLE IN DATA PROTECTION? AN ANTI-RACIST PERSPECTIVE FOR TECH

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by European Network Against Racism (ENAR) (BE)
Moderator Oyidiya Oji, European Network Against Racism (ENAR) (BE)
Speakers Oumaima Hajri, Rotterdam University of Applied Sciences

WEDNESDAY 24 MAY 2023

and member of the Forum of European Muslim Youth and Student Organisations (FEMYSO) (NL); Naomi Appelman, Institute for Information Law (University of Amsterdam) and member of Racism & Technology Center (NL); Osama Al Sayad, Arabi Facts Hub (EG); Tebogo R. Mazibuko, Compliance, data protection and digital ethics (ZA)

Privacy and data protection are only affordable for a few. People with different lived experiences are often included in those concepts without acknowledging their backgrounds. Tech must recognise and embrace diversity for a better outcome that respects and honours alternative knowledge and history. It is important to create an environment for exploring the safety, privacy and data especially for those who historically never took them for granted.

- What is the experience with privacy and data protection for vulnerable groups?
- How can we make sure that their privacy is valued this time?
- What does it mean to protect the data privacy of marginalised communities?
- How can technology be reimagined without harming these communities? Can an anti-racist perspective be the solution?

18:30 – COCKTAIL SPONSORED BY EDPS

in Le Village

CPDP2023 WORKSHOPS AT M-VILLAGE GRANDE

08:30 - WELCOME AND INTRODUCTION BY PAUL DE HERT in Grande Halle

08:45 – Workshop WHEN DATA PRIVACY MEET CORPORATE MORALITY: SHOULD DATA PROTECTION BE PART OF CORPORATE SOCIAL RESPONSIBILITY?

Organised by CMS (BE)
Workshop facilitator Tom De Cordier, CMS (BE)
Speakers Isabelle Vereecken, European Data Protection Board (EDPB) (EU); Irene Pollach, Aarhus University (DK); Emmanuelle Bartoli, Capgemini (BE)

New and enhanced forms of digital communication (social media platforms, digital advertising infrastructures, cross-media tracking) offer companies access to vast amounts of valuable data about the behaviors, habits and preferences of their current and prospective customers and employees. This creates new demands for corporate social responsibility, given that enhanced digital technologies may affect individuals' ethical rights to privacy, consent, and self-determination in new ways. Since the law typically lags behind new technological possibilities and the ethical considerations associated with them, it is often a question of corporate morality to what extent companies use people's digital data to further their business interests and with what level of detail they make their processing of data transparent. Companies are increasingly pressured to embed privacy concerns into their corporate social responsibility agendas, which can potentially lead to a competitive advantage over less privacy-compliant companies.

- What are the pros and cons of building data protection into your CSR program?
- When does it make sense to build in data protection into your CSR program?
- How to integrate data protection into your CSR program?

10:00 - COFFEE BREAK

10:30 – Workshop ADVANCED DATA PROTECTION CONTROL (ADPC): A FUNDAMENTAL TRANSFORMATION IN PRIVACY PRACTICES

Organised by Sustainable Computing Lab, Vienna University of Economics and Business (AT) and NOYB (AT)
Workshop facilitator Harshvardhan J. Pandit, Dublin City University (IE)
Speakers Max Schrems, NOYB – European Center for Digital Rights (AT); Soheil Human, Sustainable Computing Lab, Vienna University of Economics and Business (AT); Alan Toner, Policy and Data Protection Expert (IE/DE)

Do you hate "cookie banners" too? Advanced Data Protection Control (ADPC) is an automated mechanism for the communication of users' privacy decisions that allows users to set their privacy preferences in their browser, plugin, or operating system and communicate them in a simple way – limiting friction in user interaction for providers and users alike, as foreseen or planned in various innovative laws. It aims to empower users to protect their online choices in a human-centric, easy, and enforceable manner. ADPC also supports online publishers and service providers to comply with data protection and consumer protection regulations. In this workshop, in a highly interactive set-up, we will introduce ADPC and reflect on the future of data protection and privacy through the lenses of ADPC, which can drive the online world towards a fundamental data protection transformation, and discuss the opportunities and challenges we face. We will also assess the prospects for browser based controls in the context of the ongoing ePrivacy negotiations, the European Commission's Cookie 'Pledge' initiative, AND developments in California under the CCPA/CPRA.

11:45 – Workshop THE (ARTIFICIAL) RIGHT TO EFFECTIVE REMEDY: EFFECTIVE REMEDY AND CITIZEN COMPLAINTS REVISITED

Organised by AI4BELGIUM
Workshop facilitator Nele Roekens (AI4Belgium, Unia)
Speakers Nicolas Deffieux, PEReN; Francesca Fanucci, ECNL/CINGO; Pierre Dewitte, CITIP

Citizens often have no idea when AI is being used that might affect them, and when citizens are aware, they do not know how and to what institution or court they could complain about the individual, collective or societal harm that arises or might arise. It is widely accepted that the right to effective remedy is negatively affected by AI legal issues such as the lack of algorithmic transparency, the lack of contestability, liability issues related to damage caused and lack of accountability for harms. Whilst recognizing the work carried out in the AI law space, a lot remains to be done.

This workshop will revisit the right to effective remedy in the digitized world with a focus on AI systems. An interdisciplinary panel will be asked to examine concrete use-cases. A debate will ensue on the pros and cons of existing and future (legal)tools to ensure meaningful effective redress. Participants will be invited to share their view on what is needed. This workshop aims to advance the discussion, which is important given the gravity of the impacts of AI technologies, particularly on vulnerable individuals and groups. The following questions will be addressed:

- What is the right to effective remedy and how is it affected in a digitized world?

  For the second part of the Q: we would ask the panelist to demonstrate this by walking us through a concrete example e.g. how could a citizen seek redress for harm caused by manipulation by a chatbot, a discriminatory hiring decision,...

Sub question: How can citizens invoke their right to effective remedy to addresscollective or societal harm that arises from the use of AI?

- Is the right to effective remedy currently foreseen in the upcoming legislative frameworks such as the EU AI Act and CoE Convention on AI, Human Rights, Rule of Law and Democracy that aim to guarantee the right to an effective remedy?
- What are existing best practices on a national level to ensure the right to effective remedy? Mandatory AI registry's + HRIA (NLD), safeguards for independency of enforcement authority (CNIL FRANCE)
- How can the right be enforced on a national level? What institution is best suited to address complaints: judiciary, market surveillance authorities/national supervisory authorities?

13:00 - LUNCH

14:15 – Workshop AUTOMATED ENFORCEMENT OF THE GDPR AND OTHER DIGITAL RIGHTS- CAN LEGAL TECH BE A SOLUTION?

Organised by NOYB (AT)
Workshop facilitator Max Schrems, NOYB (AT) & Stefan Schauer, NOYB (AT)

Enforcement of all digital rights can be a difficult task, considering the large number of violations and the limited resources of regulators. The talk will give a deep dive into the systems developed by noyb to identify, contact and litigate more than 700 cookie banners in the EU. We share how innovative legal tech and IT tools can help the regulators, civil society and litigators to enforce digital rights efficiently, with a large scale impact that could change the market's behaviour.

- Which cases are suitable for automated enforcement action?
- Which options exist to streamline cases, such as automatic settlements of cases?
- How can public or private organizations manage large case loads?
- What are the dangers of automated enforcement?

15:30 - COFFEE BREAK

16:00 – Workshop DATA PROTECTION IN THE EU REGULATION ON POLITICAL ADVERTISING: A NEW PARADIGM?

Organised by European Partnership for Democracy (EPD) (BE)
Workshop facilitator Fernando Hortal Foronda, European Partnership for Democracy (EPD) (BE)
Speakers Anna Colaps, EDPS (EU); Anna Julia Donáth, Member of the European Parliament (EU); Maria-Manuel Leitão-Marques, Member of the European Parliament (EU); Asha Allen, CDT Europe (EU)

The aim of the session is raising awareness among the privacy community of the upcoming regulation on political advertising in the EU for the implications that it has for the regulation of behavioural advertising beyond political advertising and for the regulation of political campaigning online globally. The session will start with brief presentations by regulators, legislators and civil society representatives working on the file and be followed by a discussion fed primarily by questions from the audience.

- What is the position of the European Parliament on personal data and political advertising and which are the assumptions underpinning it?
- How do rules that restrict processing of personal data interplay with rules on the transparency of political advertising?
- How will rules on personal data in this regulation relate to the DSA and the GDPR, as well as to future EU regulations?
- How to simultaneously protect freedom of expression and privacy in political advertising?

17:15 – Workshop RIGHT TO DIGITAL INTEGRITY - A NEW FRAMEWORK FOR DATA PROTECTION

Organised by Nym Technologies (CH)
Workshop facilitator Alexis Roussel author of "Our precious digital integrity" and COO of Nym Technologies and Harry Halpin, CEO of Nym Technologies
Speakers Johan Rochel; Lusine Vardanyan; Alexander Barclay, Canton of Geneva (CH); Catherine Lennman, Swiss Federal Data Protection (CH)

The panel will introduce the notion of "Right to digital integrity" as a new approach to data protection, focusing on individual autonomy and security in the digital realm. The framework does not take the commodification of data as an inevitability and thereby goes one step further than the GDPR in furthering digital self-determination. This principle has been voted by the Geneva Parliament to be added in the local Constitution as part of fundamental rights with the Right to Life. The debate is now also

WEDNESDAY 24 MAY 2023

at the Swiss Federal Parliament. The workshop will discuss these cases and the potential practical implications of its adoption.

18:30 – COCKTAIL SPONSORED BY EDPS

in Le Village

CPDP2023 WORKSHOPS AT M-VILLAGE MIDI

08:30 - WELCOME AND INTRODUCTION BY PAUL DE HERT in Grande Halle

08:45 – Workshop INTERNET SHUTDOWNS – ARE INTERNET BLACKOUTS EVER JUSTIFIED?

Organised by LSTS (BE)
Workshop facilitator Johannes Thumfart, LSTS (BE), HWR Berlin (DE)
Speakers Nishant Shah, Chinese University of Hong Kong / Harvard University (CH/UK); Kris Ruijgrok, University of Amsterdam / Leiden University (NL)

Internet shutdowns (ISs) are intentional disruptions of internet access by governments and/or private controllers of internet access within a specific location and often limited to specific apps. In 2022 alone, there were 187 Internet shutdowns globally, 184 in 2021, 159 in 2020. The number of countries enacting ISs has been rising steadily. India, the world's largest democracy with authoritarian features, is, by far, leading the statistics. Western democracies, too, have enacted them, for example, GB in 2019, Spain in 2017, the US in 2011. Focussing on India, the participants discuss ISs from the perspective of the underlying conflict of rights, norms, values, and the security aims of governments and consider the responsibilities of private ISPs.

10:00 - COFFEE BREAK

10:30 – Workshop TRUSTWORTHY (RE)USE OF HEALTH DATA ENDORSED BY EHDS

Organised by The European Institute for Innovation through Health Data (i~HD) (EU)
Workshop facilitator Jens Declerck, i~HD
Speakers Christophe Maes, NVIDIA (US); Maria Christofidou, i~HD (BE); Nathan Lea (UK)

Europe's digitalized health data ecosystem is not used to its full potential due to information governance complexities, lack of software system quality and data quality or legal barriers. The forthcoming European Health Data Space (EHDS) regulation will facilitate data flows describing the requirements to exchange and access different types of health data and to support healthcare research. During the workshop, i~HD's experts will set the scene of the most important EHDS primary and secondary health data use requirements and solutions under the spotlight of the GDPR legislation. These interactive round table discussions will tackle whether the principles and underlying processes of good practices, being used in the healthcare sector, are also able to improve information governance, data quality and system quality in other sectors, or whether the healthcare sector can learn from initiatives used in other sectors.

- Information governance
- Software system quality
- Data quality

11:45 – Workshop HOW TO DESIGN AND USE PRIVACY ICONS TO EFFECTIVELY INFORM ABOUT PRIVACY RISKS

Organised by University of the Arts Berlin / Einstein Center Digital Future (DE)
Workshop facilitator Maximilian v. Grafenstein, University of the Arts Berlin (UdK) (DE), Einstein CenterDigital Future (ECDF) (DE)
Speakers Isabel Kiefaber, University of the Arts Berlin (DE); Paul Grassl, University of the Arts Berlin (DE)

The role of legal design in the process of determining effective ways to fulfil legal transparency requirements has significantly gained in relevance. One reason for that is that with the help of UX-Design research, it becomes possible to utilise both visual and user experience design as well as empirical qualitative and quantitative research methods to determine whether a transparency measure is effective or not. In this Workshop we want to focus on the use of Privacy Icons and demonstrate how they should be designed and used to effectively supply the data subject with information about data processings (respectively their risks). The workshop builds on our research project on Privacy Icons, which has been running for almost 5 years now, and is the first publication of our results including design templates (for privacy policies and consent forms) and a Privacy Icons catalogue with around 100 icons.

- How can Icons help with effectively informing data subjects about specific privacy risks?
- How do they have to be properly designed and used with respect to the specific visual context (esp. consent forms like cookie banners and privacy policies)?

13:00 - LUNCH

14:15 – Workshop TENSIONS BETWEEN CONSUMER LAW AND PRIVACY IN THE CONTENT CREATOR ECONOMY

Organised by Utrecht University/UU (NL)
Workshop facilitator Catalina Goanta, Utrecht University (NL)
Speakers Michael Veale, UCL (UK); Anne-Jel Hoelen, Autoriteit Consument Markt (NL); Giovanni De Gregorio, Bocconi University (IT); Alessia D'Amico, UU (NL)

This workshop brings together regulators and multidisciplinary academics to reflect upon the increasing tensions arising from the commodification of identity by content creators, who need to comply with commercial obligations set out by consumer protection, while also having own expectations of privacy and publicity. In particular, the workshop will address:

- The role of influencers/creators as traders under the consumer acquis;
- The privacy implications for their commodified identity;
- The potential for reform in consumer protection information duties;
- The role of platforms as facilitators of information flows and duties to protect the privacy of their users (including creators), as well as the power they exercise over content creators (including via the DSA requirements of registration, etc).
- When are creators traders? What benchmarks are being used or are desirable to measure this?
- What privacy expectations/rights should creators have when becoming brands of their own identity?
- Are more privacy-friendly registrations for start-up creators necessary?
- What can self-regulation do about these issues?

15:30 - COFFEE BREAK

16:00 – Workshop PERSONALISED PRIVACY: HOW CAN WE LEVERAGE PERSONALIZATION FOR BETTER PRIVACY PROTECTION?

Organised by Maastricht University, Law and Tech Lab (NL)
Workshop facilitator Aurelia Tamò-Larrieux (NL), Arianna Rossi (LU)
Speakers Meihe (Iris) Xu (NL); Marie Potel-Saville (FR); Estelle Hary, CNIL, (FR)

In this hands-on workshop, we analyse the potential of personalisation for better privacy protection by envisaging a future where disclosures and data processing operations are tailored to individual needs and preferences (e.g., by means of personalised privacy assistants). Despite the growing interest in the personalisation of services from different disciplines - law, computer science, psychology, sociology - we are still lacking a comprehensive understanding of what personalised disclosure and data authorisations mean in practice, how they can be technically developed, what benefits and risks arise from it, and how to balance the ethical, legal, and societal aspects of personalisation. Through thought experiments, we will explore how personalised privacy might impact future regulatory developments and debate the benefits and downsides of personalising data processing experiences.

- Which personalisation techniques can be envisaged and leveraged to protect the privacy of end-users online better?
- What would a personalised privacy environment (e.g., mediated through personalised privacy assistants) entail in terms of individual agency?
- What paradigm shifts are needed to create personalised privacy regimes and how can we ensure accountability of such approaches?
- How can we balance social values (e.g., solidarity, uniformity) and personalised preferences within the field of privacy protection?

17:15 – Workshop WORLD CAFE: WHOSE DATA? THE NEW INDIVIDUAL AND NEW COLLECTIVE IN THE DIGITAL WORLD

Organised by University of Manchester (UK)
Workshop facilitator Rebecca Mignot-Mahdavi, University of Manchester (UK)
Speakers Beatriz Botero Arcila, Sciences Po (FR) and Berkman Klein Center at Harvard University (MA); Tobias Blanke, University of Amsterdam (NL); Gail Lythgoe, University of Manchester (UK); Fabien Tarissan, CNR and ENS Paris-Saclay (FR)

Data doubles, algorithmic subjects, digital selves. Who are the bearers of privacy rights in the digital world? Do these rights address the unique challenges that digitalization creates for individual and collective agency? Governance by data arguably disrupts the traditional concepts that shaped legal subjecthood. Yet, data protection laws and data governance rules in AI Governance projects are shaped without including these arguably new forms of legal relations. Led by a computer scientist, a philosopher, a business representative, and two academics/lawyers, this world cafe will be an opportunity to test the hypothesis that governance by data creates new (legal) subjects and to actively explore how current or future regulations could adapt to safeguard rights. The implications of such moves for our societies and modes of regulation will be the object of concluding remarks by the speakers, following the world cafe.

- The world cafe is a creative process aiming to foster collaborative thinking: it is used to stimulate dialogue in large settings, allows to generate ideas, share knowledge and stimulate innovative thinking in a short amount of time-Each cafe table will be equipped with multiple placemats on which the 'guests' will be able to scribble some notes.
- Each table will name a 'host' who will be in charge of welcoming new guests after the first exchange. All guests are travelers, and move from one table to another, carrying with them ideas that emerged from previous rounds. This travel allows for a cross-pollination process of ideas.
- At the end of these three rounds of exchanges, the hosts will summarize and report the main ideas that came out from the three rounds of exchanges. The speakers will share concluding remarks to end the session.-Who are the bearers of privacy rights in the digital world? How do these rights address the unique challenges that rising digitalization creates for individual and collective agency

18:30 – COCKTAIL SPONSORED BY EDPS

in Le Village

WEDNESDAY 24 MAY 2023

THURSDAY 25TH MAY 2023

Please note that this is a preliminary version of the programme.

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

CPDP2023 PANELS AT GRANDE HALLE

08:45 – BEST PRACTICES FOR PROTECTING CHILDREN'S PRIVACY IN THE DIGITAL AGE: THE PRACTITIONERS' PERSPECTIVE

Business ☆☆☆ **Policy** ☆☆☆
Organised by CPDP
Moderator Steward Dresner, Privacy Laws & Business (UK)
Speakers Laura Brodahl, Wilson Sonsini (BE); Ruth Boardman, Bird & Bird (UK); Joke Bodewits, Hogan Lovells (NL); Simon Mortier, McDermott Will & Emery (BE); Diletta De Cicco, Squire Patton Boggs (BE)

There remains considerable uncertainty as to how to best protect children's privacy. Data controllers and processors in the EU are thus often left in a state of confusion as to what is required of them, and as to how they ought best to meet their obligations. Against this background, this panel brings together practicing lawyers who deal with issues of children's privacy on a daily basis. Panelists will offer their perspectives on the current situation and will consider, amongst others, the following questions:

- What are the key current issues concerning the protection of children's privacy?
- What are the different approaches to dealing with children's privacy, and which novel forms of best practice have come to the fore over the past years?
- How should lawyers and other professionals deal with the ongoing uncertainty surrounding children's privacy?
- What can legal practice tell us about about policy solutions moving forwards?

10:00 - COFFEE BREAK

10:30 – IS STRONG ENCRYPTION MORE IMPORTANT NOW THAN EVER?

Academic ☆ **Business** ☆☆ **Policy** ☆☆☆
Organised by Apple (US)
Moderator Gary Davis, Apple Distribution International (IE)
Speakers Namrata Maheshwari, Access Now (IN); Erik Neuenschwander, Apple (US); Hannah Neumann, MEP (DE); Edvardas Šileris, European Cybercrime Center, Europol (EU)

Is strong encryption more important now than ever? New regulatory efforts and rising cybersecurity threats are exerting increasing pressure on businesses and Governments to answer this question. Until now, security experts from industry and civil society have responded with a resounding Yes – that strong encryption protects everyone from harm and threats. Their view is that any form of bypassing would require weaker encryption, resulting in new vulnerabilities that could be exploited by anyone, anywhere. Regulatory efforts influencing this debate, although not intended to undermine encryption, perhaps rest on the assumption that businesses have enough resources to create technology that will solve the complex issue of maintaining strong encryption while responding to legislative expectations. These developments have caused businesses to publicly announce their concerns that strong encryption may be in danger. In this panel, we seek to revisit this pressing debate considering the latest developments in encryption technology and emerging regulatory and security needs.

- Is there a real threat to encryption today?
- Can legitimate policy goals that may impact strong encryption be balanced with privacy and data protection rights?
- What are the technical limitations that might be considered that support the view that strong encryption cannot have vulnerabilities built into it?
- Are there options that should be considered for protecting citizens without building vulnerabilities into encryption?

11:45 – CONVERGENCE IN ACTION: COOPERATION THROUGH NETWORKS – FROM THE REGIONAL TO THE GLOBAL DIMENSION

Academic ☆ **Business** ☆ **Policy** ☆☆☆☆
Organised by European Commission (EU)
Moderator Bruno Gencarelli, European Commission (EU)
Speakers Michael McEvoy, Information and Privacy Commissioner for British Columbia, representing the Asia Pacific Privacy Authorities (APPA) Forum; Josefina Roman Vergara, Commissioner of Mexico's National Institute for Transparency, Access to Information and Personal Data Protection (INAI), representing the Ibero-American Data Protection Network (RIPD)

Regional networks of data protection authorities (DPAs) have emerged as key actors on the international privacy scene. Uniquely placed to create synergies beyond the traditional bilateral dimension of cooperation, they bring a "critical mass" of regulators working together not only on enforcement but also on developing shared interpretation of privacy concepts and common compliance tools such as the model contractual clauses for cross-border transfers adopted by the Ibero-American Data Protection Network (RIPD).

At last year's CPDP, the panel organised by the European Commission discussed the benefits and outcomes of cross-border cooperation between DPAs at the regional level. This year, we propose to explore how DPA networks can cooperate at the global level, as they grapple with similar challenges and opportunities.

This high-level panel will bring together representatives from the European Data Protection Board (EDPB), RIPD, the Network of African Data Protection Authorities (NADPA/RAPDP) and the Asia Pacific Privacy Authorities (APPA) Forum. It will explore the potential of such global, inter-network cooperation, together with concrete examples and case studies.

- What tangible examples of 'cross-fertilization' exist (such as the use/adaptation of guidance or compliance tools adopted in the context of other regional networks, e.g. use in the EU of the anonymization guide and tool developed by the Singaporean DPA, the development of "bridges" between regional model clauses for transfers, etc.) and how might we build on them?
- What should be the priority areas on which such inter-network cooperation should focus?
- Is it time to structure cooperation between regional networks? A network of networks?

13:00 - LUNCH

14:15 – THE FUTURE OF EFFECTIVE ENFORCEMENT

Academic ☆ **Business** ☆ **Policy** ☆☆☆☆
Organised by European Data Protection Supervisor (EU)
Moderator Wojciech Wiewiórowski, European Data Protection Supervisor (EU)
Speakers Andrea Jelinek, Austrian Data Protection Authority & European Data Protection Board (EU); Olivier Micol, European Commission (EU); Ursula Pachl, BEUC (BE); Herwig Hofmann, European and Transnational Public Law at the University of Luxembourg (LU)

This panel seeks to serve as an official follow-up to the debate kick-started at the EDPS 2022 conference on the future of effective enforcement of data protection law. A year following the EDPS conference, this panel will take stock of the recent developments. Topics such as improving GDPR enforcement through the Commission's work program, major cases issued under the One-Stop-Shop model since, or recent challenges and systemic disputes that have emerged, all may be discussed. The central aim of the panel will be to answer the question of lies in store for the future of effective enforcement. This panel will be an opportunity to hear from the heart of the debate itself.

- What is the current state of initiatives undertaken to improve enforcement such as streamlining cooperation and harmonizing national procedural rules?
- How has the enforcement landscape changed over the last year? Have recent cases or soft-law approaches altered the status-quo?
- What lessons can we still learn from other fields of law, pointing to the need for a more central approach?

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

16:00 – PRIVACY THROUGH INNOVATION - PRIVACY ENHANCING TECHNOLOGIES, CONSUMER PROTECTION AND THE ONLINE ADS ECOSYSTEM

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by Google (US)
Moderator Marek Steffen Jansen, Google (US)
Speakers Anthony Chavez, Google (US); Rob van Eijk, Future of Privacy Forum (FPF) (NL); Marie-Paule Benassi, DG JUST, European Commission (BE); Stefan Hanloser, ProSiebenSat.1 Media (DE); Christian Reimsbach-Kounatze, OECD Directorate for Science, Technology and Industry (INT)

In today's digital age, privacy is a growing concern for individuals, especially regarding the tracking of their activities across various sites and applications for digital advertising. However, the emergence of Privacy Enhancing Technologies (PETs) and Privacy Preserving Technologies (PPTs) presents a unique opportunity to mitigate privacy risks, streamline legal compliance, and establish trust in digital technology. PETs and PPTs have the potential to significantly enhance consumer protection online while enabling the effective use of data through technical approaches such as data aggregation, data noising, and processing sensitive data on-device or in trusted cloud execution environments. This pane will explore the concept of privacy through innovation and the incentives required for further investment in the development and adoption of PETs. Additionally, the discussion will focus on the need for international convergence on acceptable standards to establish global, accessible, tech-neutral, and affordable PETs.

17:15 – AI FAIRNESS TESTING: MAKING IT WORK IN THE REAL WORLD

Academic ☆☆☆ **Business** ☆ **Policy** ☆☆
Organised by Uber (US)
Moderator Gianclaudio Malgieri, Leiden University (NL) & Brussels Privacy Hub (BE)
Speakers Dan Svirsky, Uber (US); Kai Zenner, European Parliament (EU); Sophia Ignatidou, AI & Data Science, Information Commissioner's Office (UK); Olivia Gambelin, Ethical Intelligence (BE/US)

There is increasing recognition that automated decision-making at scale, using AI or ML, is changing the nature of discrimination. Discrimination was once driven primarily by individuals and systemic barriers. Now, machine learning can learn from biased data. In doing so, it may amplify existing prejudice. As a result, regulators, civil society advocates, and tech companies have recognized the need for testing algorithms for bias against historically disadvantaged groups.

In this panel, we bring together practitioners from tech companies, academics, policy-makers, regulators and AI ethics advisors to provide an overview of how fairness testing works (or should work) today. A data scientist from Uber's Fairness Research team will describe how fairness testing actually works in practice. The AI ethics advisors will describe

THURSDAY 25 MAY 2023

challenges and best practices for assessing fairness tests. Policy-makers and regulators will provide their view about how existing and upcoming legislation can allow, support or encourage fairness testing.

- How does fairness testing actually work and what data and statistical methods are used?
- What are the challenges and best practices for robust fairness testing?
- Can a uniform model work across industries and use cases?
- What can regulators learn from practitioners as they craft legislation?

18:30 – COCKTAIL SPONSORED BY UBER

in Le Village

CPDP2023 PANELS AT AREA 42 GRAND

08:45 – SHARING IS CARING: BEST PRACTICES, INTERMEDIARIES AND SYNTHETIC DATA FOR DATA SPACES

Academic ☆ **Business** ☆☆ **Policy** ☆☆☆
Organised by Centro Nazionale IoT e Privacy (IT)
Moderator Carlo, Rossi Chauvenet, Università Bocconi (IT)
Speakers Evelyne Studer, eBay (US); Daniele Panfilo, Aindo (IT); Félicen Vallet, CNIL (FR); Elisabetta Biasin, KU Leuven (BE)

Sharing is caring and sharing data may be part of the answer to nowadays' issues, but its development is still in the first phase. The creation of data spaces faces obstacles and raises (personal) data protection concerns. To date, there are no proper best practices on technical and organizational measures. In light of these issues, the panel will explore solutions to create functional and safe data space and data-sharing models, analyzing the role of the data intermediaries within the sharing ecosystem. It will Focus on synthetic data, a cutting-edge privacy-enhancing technology, that promises to be a viable alternative to the use of personal data in various sectors. Sectoral data spaces developed in a framework made by synthetic data may come to solve the issues, guaranteeing citizens' rights while unleashing the potential to fully exploit the value within data.

- Are we technology-ready to govern the EU digital single market?
- Is it possible to balance the highest standards of data protection with maximum data availability?
- May a synergy between data intermediaries and synthetic data be the answer to the growing need of data?
- How can big platforms team with SMEs to create data spaces and help in solving today's problems?

10:00 - COFFEE BREAK

10:30 – TRUSTWORTHY DATA SPACES FROM THE PERSPECTIVE OF THEIR DEVELOPERS AND USERS - CURRENT CHALLENGES AND THE WAY FORWARD

Academic ☆☆☆ **Business** ☆☆ **Policy** ☆
Organised by Department of Innovation and Digitalisation in Law, University of Vienna (AT)
Moderator Hande Özkayagan-Prändl, University of Vienna (AT)
Speakers Evangelos Markakis, Hellenic Mediterranean University (GR); Velislava Hillman, ETOILE PARTNERS LTD /London School of Economics and Political Science (UK); Sebastian Steinbuss, International Data Spaces Association (DE); Alberto Berreteaga Barbero, TECNALIA (ES); Katarzyna Barud, University of Vienna (AT)

The EU's data strategy focuses on three primary objectives: the free movement of data within the EU and across sectors; respect for European rules and values, especially regarding the protection of personal data, consumer protection and competition law; fair access to and use of data with trustworthy data management. Emerging data spaces aim to achieve them by creating environments that enable data exchange compliant with legal and technical standards ensuring data security. The panel will discuss the challenges of building international and European data spaces. Based on the examples provided by International Data Spaces and the TRUSTEE project, the panellists will explore how emerging changes in the legal framework impact data spaces, what security solutions are appropriate to ensure data privacy, security, interoperability and compliance with ethical standards and how the deployment of AI/ML solutions could potentially improve data manipulation in data spaces without compromising the privacy of individuals.

- What are the main challenges involved in the design and development of data spaces, considering the legal, ethical and technological perspectives?
- How does the possibility to search and utilise data in the encrypted domain enforce data privacy in data sharing between a data provider and a data consumer?
- How can the accountability of the actions conducted by the actors using the data spaces for the data exchange and interaction be ensured?
- How might the application of the AI/ML solutions facilitate the data manipulation in thedata spaces while preserving its privacy?

11:45 – REGULATING E-MENTAL HEALTH: PROGRESS, PITFALLS AND GLOBAL LESSONS

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by IEEE Standards Association (US)
Moderator Maria Palombini, IEEE Standards Association (US)
Speakers Becky Inkster, WYSA (UK); Christopher Boyd-Skinner, Australian Commission on Safety and Quality in Health Care (AU); Maureen Abbott, Manager, Access to Quality Mental Health Services, Mental Health Commission of Canada (CA); Elisabeth Steindl, University of Vienna (AT)

Exponential growth in e-Mental Health technologies offers great promise for mental health treatment, crisis and addiction support, suicide prevention and building mental resilience. Conversely, the sensitivity of health information collected presents ethical, data protection and privacy challenges, with sector regulation remaining unclear. Jurisdictions including Australia and Canada have developed novel e-Mental Health standards and application assessment frameworks that may point the way to safer, more culturally equitable, evidence-informed innovation. Is the diverse e-Mental Health Industry, including AI-enabled technologies, ready to embrace better data governance? What are the growing efforts to digitise public mental health services? Are existing regulatory instruments swift enough to improve protections for vulnerable citizens? This exploratory panel presents an inter-jurisdictional examination on data protection and privacy challenges in e-Mental Health, aiming to share global lessons on approaches to safety, quality and improved protection of citizens' sensitive data.

- What guarantees can standards, accreditation and assessment frameworks provide to support safer delivery of digital mental health products?
- What are the challenges and barriers with hard and soft regulatory models?
- Is over-regulation a barrier for innovation and what engagement strategies are required to bring Industry onboard?
- What legal instruments do we have to respond to these challenges?

13:00 - LUNCH

14:15 – PRIVACY ENGINEERING FOR TRANSPARENCY AND ACCOUNTABILITY

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by TU Berlin (DE)
Moderator Frank Pallas, TU Berlin (DE)
Speakers Elias Grünewald, TU Berlin (DE); Katharina Koerner, International Association of Privacy Professionals (IAPP) (US); Isabel Wagner, University of Basel (CH); Suchakra Sharma, Privado (US/IN)

This panel drives an interdisciplinary discourse on the transparency and accountability principles as manifested in the GDPR. We characterize the emerging field of privacy engineering with current examples from techno-legal research, industry reports, and their critical evaluation. Doing so, we delineate as to why the current practice with regards to transparency and accountability does not unfold its potentials, which policy implications we should aim for, and how technological advances can help here. The speakers focus on the practical implementation and new forms of transparency and accountability enhancing technologies in line with the givens of large-scale IT infrastructures processing personal data. In addition, the debate will oscillate between the perspectives of data controllers and data subjects' rights and actual needs.

- What is the state of the art in effective privacy engineering for transparency and accountability?
- What are the guiding principles for their legal and technical implementation and enforcement?
- How can we support the communication between legal, technical, and supervisory data protection roles?
- How to reconcile conflicting business goals with regulatory obligations and how to enhance day-to-day compliance for everyone?

15:30 - COFFEE BREAK

16:00 – THE UNDERUSE OF PERSONAL DATA, ITS OPPORTUNITY COSTS, AND EU POLICIES

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by University of Turin (UNITO) (IT)
Moderator Ugo Pagallo, University of Turin (IT)
Speakers Alberto Di Felice, DIGITALEUROPE (IT); Bárbara da Rosa Lazarotto, VUB (BE); Antonios Bouchagiar, European Commission (EU); Aurélie Pols, Aurelie Pols & Associates (NL)

The underuse of personal data and of the related data-driven technologies represents a serious problem, namely, that which economists dub as their opportunity costs, the costs human societies pay for not using personal data and data-driven technologies, or using them far below their full potential. Whereas, in 2020, the European Parliament denounced such underuse as a major threat, several initiatives of the Commission, e.g. the Data Governance Act, intend to tackle the phenomenon, by providing a regulatory framework for novel data intermediaries, data-sharing infrastructures and by encouraging the sharing of data for commercial and altruistic purposes. The aim of the panel is to shed light on these initiatives and how they relate to principles and provisions of the GDPR.

- What triggers the underuse of personal data and of the related data-driven technologies?
- What are the fields in which such underuse is more threatening?
- What are the strengths and weaknesses of current EU policies against the underuse?
- How could we improve these policies?

17:15 – CONNECTING GLOBAL PRIVACY FRAMEWORKS TO ENABLE TRUSTED DATA FLOWS

Academic ☆ **Business** ☆☆☆ **Policy** ☆☆
Organised by Workday (US)
Moderator Isabelle Roccia, IAPP (BE)
Speakers Bruno Gencarelli, International Affairs and Data Flows, European Commission (EU); Barbara Cosgrave, Workday (US); Clarisse Girot, Data Governance and Privacy Unit, OECD (INT); Manon Habets, Linklaters (BE)

The global privacy landscape continues to accelerate with new laws introduced, updated or coming into effect in the last two years. The U.S. continues it slow but consistent approach towards comprehensive privacy legislation, while the EU advances with its procedure to adopt the EU-U.S. Data Privacy Framework. OECD countries have adopted a Declaration on Government Access to Personal Data, while the Global CBPR

THURSDAY 25 MAY 2023

Forum was established to boost multilateral cooperation in promoting trusted global data flows. In the midst of these efforts, regional and national data sovereignty approaches are becoming more prominent.

This panel will explore the latest in privacy rules and trends worldwide, where they align or differ and where tensions and uncertainty exist. It will also examine how cooperation between different regions can be strengthened to foster synergies in privacy standards and boost cross-border data flows.

- Is the need to connect global privacy frameworks to enable trusted data flows compatible with the emergence of regional and national data sovereignty ambitions?
- Does the EU-U.S. Data Privacy Framework sufficiently address the issues found lacking by the CJEU in Schrems II to withstand a legal challenge?
- What impact will the OECD Declaration on Government Access to Personal Data have to improve trust in cross-border data flows?
- How are global businesses addressing the challenges of complying with multiple laws during these challenging economic and geopolitical times?

18:30 – COCKTAIL SPONSORED BY UBER

in Le Village

CPDP2023 PANELS AT AREA 42 MIDI

08:45 – BRIDGING THE GAP – ENFORCING THE DMA, LEARNING FROM THE DATA PROTECTION EXPERIENCE

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by ARTICLE 19
Moderator Johnny Ryan, Irish Council for Civil Liberties (ICCL) (IE)
Speakers Maria Luisa Stasi, ARTICLE 19 (UK)

To establish fairness and contestability in digital markets for business and end users alike surely requires to deal with how personal data are gathered, processed and used by the various actors. Indeed, the Digital Markets Act contains a number of provisions that overlap and interplay with data protection rules, and in particular with the General Data Protection Regulation. Examples include data portability obligations (Article 6(9)), and the requirement to obtain end user consent to comply with certain DMA obligations (Articles 5{2}) and 6{10}).

An adequate enforcement of this new regulatory framework will thus need an informed, cross-disciplinary, constructive regulatory dialogue and exchanges with relevant regulators, experts and stakeholders on such interplay, with the aim to guarantee the well-functioning of the data economy, as well as an effective data protection.

- What are the data protection implications of the DMA?
- How can we bridge the DMA and the GDPR?
- What should be the enforcers' priorities?
- What role does the protection of privacy and other end users' fundamental rights play in the enforcement of DMA rules?

10:00 - COFFEE BREAK

10:30 – NEW EU DIGITAL LEGISLATION AND ITS IMPACT ON THE ROLE OF SUPERVISORY AUTHORITIES AND DPOS

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by European Federation of Data Protection Officers (EFDPO) (EU)
Moderator Pierre-Yves Lastic, European Federation of Data Protection Officers (EFDPO) (EU)
Speakers Judith Leschanz, Privacyofficers.at (AT); Mgr.František Nonnemann, Association for the Protection of Personal Data (Spolek pro ochranu Osobních údaju) (CZ); Michael Will, Bavarian State Office for Data Protection Supervision (DE)

The new EU digital legislation (Artificial Intelligence Act, Digital Services Act, Digital Markets Act, Data Governance Act, Data Act and the various European Data Spaces) introduces new instances of regulation in the field of data economy and data protection. What is or could be the role of data protection officers and supervisory authorities in this constellation? This panel tries to give an overview of the views of the EU regulatory bodies as well as of the data protection officers themselves.

- What is or could be the role of European and national supervisory authorities in respect to new and emerging EU digital legislation?
- What is or could be the role of data protection officers in respect to new and emerging EU digital legislation?
- Will the role and responsibilities of the authorities supervising digital services and markets, artificial intelligence and data protection be harmonized throughout Europe?
- Should the role and function of the DPO be expanded to adapt to these new legislative circumstances?

11:45 – HOW DEMOCRACIES PROTECT BOTH PRIVACY AND NATIONAL SECURITY

Academic ☆☆ **Business** ☆ **Policy** ☆☆☆
Organised by American University (US)
Moderator Alex Joel, Tech, Law and Security Program, American University Washington College of Law (US)
Speakers Audrey Plonk, OECD (US); Steve Wood, PrivacyXConsulting / Allen and Overy (UK); Aisling Kelly, Microsoft (IE); Christian Wiese Svanberg, Danish Defense Intelligence Service (DK); Thorsten Wetzling, Stifting Neue Verantwortung (DE)

For the past decade, participants in international discussions regarding cross-border data flows have raised serious concerns about national security and law enforcement access to personal data held by the private sector. In December 2020 the OECD established a drafting group comprised of government representatives with expertise in data protection, national security, and law enforcement, to identify commonalities in how democratic nations—in contrast with authoritarian regimes—protect both privacy and national security when accessing personal data from the private sector. Two years later, this effort culminated in the landmark Declaration on Government Access to Personal Data Held by Private Sector Entities. This panel of experts who participated closely in how the OECD process will discuss key aspects of the Declaration and its implications for building trust in cross-border data flows.

- What are the most important aspects of the OECD Declaration?
- In what way are the principles for law enforcement and national security access different from other data protection principles, and why?
- What can we learn from the intensive two-year effort to identify these principles?
- What are the implications of the Declaration for the future of data flows?

13:00 - LUNCH

14:15 – (MIS)USE OF SURVEILLANCE TECHNOLOGIES AS EMERGENCY MEASURES: GLOBAL LESSONS FROM THE COVID-19 PANDEMIC

Academic ☆☆ **Business** ☆ **Policy** ☆☆☆
Organised by International Network of Civil Liberties Organizations (INCLO) (CH)
Moderator Karolina Iwańska, European Center for Not-for-Profit Law (ECNL) (NL)
Speakers Martin Mavenjina, Transitional Justice at the Kenya Human Rights Commission (KE); Bastien Le Querrec, La Quadrature du Net (FR); Rosamunde van Brakel, Vrije Universiteit Brussel (BE); David Reichel, EU Fundamental Rights Agency (EU)

More than half the world's countries, including EU Member States, have enacted emergency measures in response to the Covid-19 pandemic. A significant aspect of governments' emergency responses has been a rapid and unprecedented scaling up of their use of technologies to enable widespread digital contact tracing and surveillance. Three years after the start of the pandemic, now is the time to take stock. This panel seeks to understand what actually occurred after the surveillance measures were first introduced, beyond the initial wave of media coverage. Speakers from civil society, EU agencies and academia will reflect on the efficacy and proportionality of pandemic-related surveillance measures and their impact on human rights globally. We will also determine what lessons have been learned so that governments, civic actors and companies are better prepared for future health or other emergencies.

- What were the impacts of pandemic-related surveillance measures on human rights and civil society globally?
- How can emergency measures be abused by governments and companies?
- What happened to the many surveillance measures adopted during the pandemic?
- What lessons can we draw for future health or other emergencies?

15:30 - COFFEE BREAK

16:00 – WHEN PRIVACY BECOMES POLITICAL

Academic ☆☆ **Business** ☆ **Policy** ☆☆☆
Organised by Datatilsynet (DK)
Moderator Kari Laumann, Norwegian Data Protection Authority (NO)
Speakers Frederik Zuiderveen Borgesius, Radboud University (NL); Patrick Breyer, MEP for the German and the European Pirate Party (DE/EU); Anna Fielder, EDRi (European Digital Rights) (EU)

While the EU is launching data strategies and regulations at a pace it is difficult to keep track with, the opposite seems to be the case at the national level in many European countries. A Privacy Commission set down by the Government in Norway recently stressed that digitalisation is happening at the expense of privacy, and that politicians largely shun the topic of privacy in policy development, referring it to celebratory speeches and platitudes. The Commission calls for a political strategy to make sure that policy development is in line with societal values and fundamental human rights.

In this workshop, a panel of experts will discuss the following questions:

- Does the EUs active stance on the use of data paralyse national governments from taking action?
- Is there a need for political action at the national level? If yes, in what areas? And how much room for manoeuver is there for European governments in an area heavily regulated by EU?
- Why has privacy largely been a politically ignored topic? What does it take for politicians to become engaged? Is a scandal needed?
- Do people care about privacy? What do they expect from their national politicians in this area?

We also invite the audience to partake in the discussion.

17:15 – DECEPTIVE DESIGN IN ONLINE INTERFACES AND SYSTEM ARCHITECTURE: QUESTIONS FOR EU LAW

Academic ☆☆ **Business** ☆ **Policy** ☆☆☆
Organised by ALTI - VU Amsterdam (NL)
Moderator Mark Leiser, ALTI, VU Amsterdam (NL)
Speakers Harry Brignull, Smart Pension (UK); Ailo Ravna, Norwegian Consumer Council (NO); Silvia De Conca, Vrije Universiteit Amsterdam (NL); Martin Husovec, London School of Economics (UK)

Designers deploy deceptive design (dark patterns) across online interfaces and system architectures. Such designs aim to manipulate users into making decisions that go against their interests or interfere with their autonomy. If deceptive design is combined with profiling, emotion recognition, recommender systems or the IoT, it can have a significant impact on individuals and society-at-large. Several provisions from the EU's consumer and data protection regimes mitigate some of the associated risks of deceptive design. New EU legislation (DSA, DMA, & AI Act)

THURSDAY 25 MAY 2023

could further regulate deceptive design. While fundamental rights can help identify deceptive forms of design, it is unsettled whether they can play a larger role addressing the associated harms. This panel contextualises deceptive design through the lenses of regulation and fundamental rights, while offering insights into how the EU's digital design acquis could be enforced to fight online manipulation.

- Is the emerging legal regime of the EU for regulating digital design (e.g. DSA, UCPD, GDPR, AI Act) sufficient to regulate manipulation?
- How do we develop a test for courts to determine if users are affected by the use of deceptive design or in the alternative, should regulators embrace the development of a legal test to determine online manipulation?
- What is the relationship between profiling and deceptive design, and how does this relationship affect the regulation of deceptive design?
- What is the role of fundamental rights in regulating deceptive design?

18:30 – COCKTAIL SPONSORED BY UBER

in Le Village

CPDP2023 PANELS AT LA CAVE

08:45 – GUARDIANS OF ETHICAL AI

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by KU Leuven Digital Society Institute (BE)
Moderator Rob Heyman, imec-SMIT-VUB (BE)
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)

With the GDPR, AI Act, and DSA, Europe has introduced important new legislation for governing the digital realm. However, developing the necessary literacy to understand morally acceptable actions and decisions in this area are not yet established. Infrastructures for assessment, oversight, and enforcement are not yet effectively in place. There is a need for a specific profession of digital ethicists who can implement good governance and conduct for AI and data practices. Already, organisations are creating positions for data ethics and responsible AI. But a formal education for this profession is still missing despite an obvious need for this expertise. Combining perspectives from industry, public management and academia, this panel asks which skills such a digital ethicist would need, and how they would develop effective agency within organisations to develop socially responsible, innovative and meaningful AI and big data practices.

- Aphra Kerr, Maynooth University / ADAPT Research Centre (IE)
- Ivonne Jansen-Dings, Province of South Holland,(NL)
- Joost Gerritsen, AI & Privacy Lawyer at Legal Beetle (NL)
- Olivia Vereha, Commit Global (RO)

10:00 - COFFEE BREAK

10:30 – THE GLOBAL HARMS OF POWERING ARTIFICIAL INTELLIGENCE – TOWARDS A SUSTAINABLE FUTURE OF DATA USE AND GOVERNANCE

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by AlgorithmWatch (DE)
Moderator Fieke Jansen, University of Cardiff (UK)
Speakers Sebastián Lehuedé, University of Cambridge (UK); Anne Mollen, AlgorithmWatch (DE); Kim van Sparrentak, European Parliament (EU); Katrin Fritsch, The Green Web Foundation (DE)

Artificial Intelligence relies on data. Currently, we see a "bigger is better" mentality in both AI research and AI business models. This leads to ever more complex AI systems and massive data sets. But are they sustainable? Currently, the ensuing environmental, social and economic harms are ignored both by established data governance regimes and regulatory approaches such as the DSA/DMA, Data Act or AI Act. We have yet to find data governance approaches that adequately respond to the unsustainability of extractivist AI data collection and data processing and their underlying technical infrastructures. In this panel, we will discuss the global harms of AI systems and shortcomings of established data governance approaches, as well as new ideas for regulations geared towards more sustainable data governance and AI policies in an age where Artificial Intelligence is becoming a general-purpose technology.

- What are global harms of data infrastructures?
- How are European data and AI governance approaches adressing sustainability aspects?
- How can AI and data governance adequately reflect environmental, social and economic sustainability?
- How to bring digital rights and sustainability actors together to pursue sustainable data governance?

11:45 – TITLE TO BE CONFIRMED

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by Mozilla
Moderator TBC
Speakers TBC

13:00 - LUNCH

PRESS CONFERENCE OF THE EUROPEAN DATA PROTECTION BOARD: PRESENTING THE NEW EDPB CHAIR

Organised by the European Data Protection Board (EU)
Speakers Andrea Jelinek, outgoing EDPB Chair, & new EDPB Chair (TBC)

On May 25th 2023 - exactly 5 years after the entry into application of the GDPR - the European Data Protection Board (EDPB) will elect its new Chair. During the press conference, the new EDPB Chair will be presented to the public and the main goals for the mandate will be discussed. Outgoing Chair Andrea Jelinek will also take some time reflect on her mandate as the very first Chair of the EDPB. After a brief presentation, members of the press and the public will be able to ask questions.

14:15 – REGULATING ACCOUNTABILITY IN COMPLEX AI VALUE CHAINS: RESEARCH COLLABORATION, TEXT AND DATA MINING, AND OTHER POSSIBLE TRAPS

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by Microsoft (US)
Moderator Lorelien Hoet, Microsoft (BE)
Speakers Natali Helberger, University of Amsterdam (NL); Peter Cihon, GitHub (US); Kris Shrishak, Irish Council for Civil Liberties (ICCL) (IE); Christoph Schuhmann, LAION (DE)

Today, AI models are often trained in multi-stakeholder research collaborations among companies, academics, and individual developers. AI models are increasingly shared publicly and hosted on platforms like GitHub and HuggingFace. These models are then often leveraged into development and deployed. Regulations that assume AI R&D is done by a single actor or single type of actor might be poorly fit for purpose. Many countries have introduced exceptions for certain text and data mining or are considering doing so.

- What does AI R&D look like today, who are the actors involved, and how do they collaborate?
- How can we ensure that policymakers get a clearer picture of AI R&D practices?
- How are text and data-mining exemptions to copyright law relevant in AI R&D?
- What are key challenges and opportunities in setting these rules of the road for AI?

15:30 - COFFEE BREAK

16:00 – ASSESSING THE IMPACT OF [ALGORITHMIC] IMPACT ASSESSMENTS

Academic ☆ **Business** ☆☆ **Policy** ☆☆☆
Organised by Electronic Privacy Information Center (EPIC) (US)
Moderator Ben Winters, EPIC (US)
Speakers Gemma Galdon Clavell, ETICAS (ES); Janneke Gerards, Utrecht University (NL); Calli Schroeder, EPIC (US); Charles Albert Helleputte, Squire Patton Boggs (BE)

Impact Assessments are a popular answer to transparency and accountability problems with algorithms, yet they remain inconsistently defined and enforced. This panel will explore different approaches jurisdictions have taken, discuss the value of these instruments, and discuss paths forward.

- What should comprise an impact assessment and what is their purpose? Does it change when required for the public and private sectors?
- How do you consider different proposals to put the onus on the business vs. independent – what the trade offs are for a regime that requires both?
- What segments of an impact assessment should be made public? How do they work with other transparency or accountability mechanisms required in a jurisdiction? Can impact assessments be used as a tool for accountability?
- In what contexts, if at all, are they actually appropriate? Can they be designed so they're not easily circumvented?

17:15 – E-COMMERCE AND DATA TRANSFERS: A LATIN AMERICAN PERSPECTIVE

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by Center for Technology and Society at FGV (BR) and European Commission (EU)
Moderator Nicolo Zingales, CTS-FGV (BR)
Speakers Pablo Palazzi, Allende & Brea, Future of Privacy Forum (AR); Samantha Oliveira, Mercado Livre (BR); Miriam Wimmer, ANPD (Brazilian Data Protection Authority) (BR); Rodrigo Polanco, World Trade Institute (CL); Alisa Vekeman, European Commission (EU)

With the increase in Internet penetration and technological advancement, e-commerce is rapidly growing in Latin America. The COVID pandemic contributed to accelerate this process in the region, boosting the growth of the Latin American market by 38%, and bringing more than 10 million consumers to make their first online purchase in 2020. At the same time, the Latin American tech sector still lags behind its international counterparts, accounting only for 3.8% of GDP. This suggests that the scaling of e-commerce will often depend on the use of technologies (such as cloud architectures) that are sourced from other jurisdictions, typically implicating international data flows, and raising questions of compliance with data protection law. In addition, data transfers in e-commerce may occur between data controllers and foreign providers of added-value services (such as analytics or productivity software) that help making effective use of collected data. This panel will explore the main regional approaches to data transfers, including the mechanisms chosen by national legislation, the emerging technological or market solutions, and the international effort to harmonize the existing framework.

- Latin American countries have a variety of different solutions in the regulation of data transfers. What are the latest developments at the regional and national level?
- Does e-commerce raise any particular challenges for data transfers regulation, and would a sector-specific approach be warranted?
- What is the impact of GDPR, and in particular the Schrems II decision by the European Court of Justice, on Latin American data transfers?
- Are international trade agreements an appropriate tool to promote a balanced and uniform approach to data transfers in the region?

THURSDAY 25 MAY 2023

18:30 – REGULATION OF ARTIFICIAL INTELLIGENCE AND PERSONAL DATA IN BRICS COUNTRIES

Academic ☆☆ **Business** ☆ **Policy** ☆☆☆
Organised by Center for Technology and Society at FGV (BR)
Moderator Luca Belli, CTS-FGV (BR)
Speakers Laura Schertel Mendes, CEDIS-IDP, Brazilian Senate Jurists Commission (BR); Ekaterina Martynova, Higher School of Economic (RU); Smriti Parsheera, CyberBRICS Project (IN); Wei Wang, CyberBRICS Project (CN); Sizwe Snail, Snail Attoneys / Mandela University (ZA)

Artificial intelligence (AI) technologies are being employed for a wide range of purposes in the BRICS countries (Brazil, Russia, India, China and South Africa). These technologies present opportunities to achieve faster and better results in different activities. However they also present risks to fundamental rights and liberties, especially the right to non-discrimination, privacy and data protection. These risks and opportunities call for regulatory action, which is being developed or is already deployed by all BRICS countries at the moment.

The panel plans to discuss the different normative initiatives regarding the regulation of AI, discussing opportunities, challenges and limits for these actions. The speakers will address the Brazilian draft AI bill, which was proposed by the Jurists Commission from the Brazilian Senate specialists. The panel will also address and evaluate the Russian AI Law, that determines a differential legal framework for the use of AI technologies until 2025, and the Chinese regulatory framework, that sets rules about the use of AI on different stages of development, bringing obligations for instance for the registry of algorithms. The panel will also discuss Insian and South African regulatory initiatives, highlighting what should be updated in the existent regulations and comparing the different approaches.

- What are the main challenges in the artificial intelligence regulation?
- What are the benefits of a risk-based approach regulation?
- What are the positive and negative highlights of the already existing normative schemes in the BRICS countries?
- What are BRICS countries approaches in terms of enforcement of AI regulations?

18:30 – COCKTAIL SPONSORED BY UBER

in Le Village

CPDP2023 PANELS AT AREA 42 PETITE

08:45 – ADDRESSING RISKS IN EMERGING LEGISLATIVE INITIATIVES AND ENGINEERING DATA PROTECTION (AND SECURITY) MEASURESS

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by ENISA (EU)
Moderator Prokopios Drogkaris, ENISA (EU)
Speakers Isabel Barberá, BitnessWise (NL); Kim Wuyts, DistriNet - KU Leuven (BE); Meiko Jensen, Karlstad University (SE); Anna Lytra, European Data Protection Board (EU)

Recent legislative initiatives have broadened our understanding of processing operations. New entities such as data intermediaries are introduced along with new concepts such as data spaces and data altruism. How do all these relate to the GDPR principles and what are the necessary steps to identify the level of risk for data subjects and how to address it. The discussion will aim to cover:

- Existing approaches on analyzing data protection risks
- Newly introduced concepts under AI Act, DGA etc
- Approaches on engineering data protection into practice

10:00 - COFFEE BREAK

10:30 – TECHNICAL STANDARDS AND THE AI ACT: LEGITIMATE AND SUFFICIENT?

Academic ☆ **Business** ☆ **Policy** ☆☆☆☆
Organised by ADAPT Centre at Trinity College Dublin (IE)
Moderator Dave Lewis, ADAPT Centre, Trinity College Dublin (IE)
Speakers David Filip, ISO/IEC JTC1 SC42 Trustworthy AI workgroup Convener, Huawei (CZ); Salvatore Scalzo, DG CNECT, European Commission (BE); Natalia Giorgi, European Trade Union Confederation (BE)

Core elements required. for the implementation of the EU AI Act involve harmonised technical standards related to risk, quality, data management, testing and verification. Some standards suitable for certifying AI system are under-development internationally by expert committees such as ISO/EC JTC1 SC42 on AI, while European Standard bodies including CEN/CENELEC JTC21 on AI are addressing how such standards can serve as harmonised standards for the Ai Act.

This raises several concerns around: the legitimacy of such standards development in bodies dominated by experts from large multinationals; whether the level of societal stakeholder involvement in this technical rule making is sufficient to protect fundamental rights; and how well can standardised technical rules can be effective across different high-risk AI applications and across different member states' enforcement of the AI Act.

4 questions that will be addressed by the panel:

- How well prepared are the bodies that will undertake AI certification and market surveillance for technical enforcement for protection of established fundamental rights?
- How can legitimacy and democratic oversight of AI rule-making be effectively extended to the development of standards by experts from multinationals in international committees?
- How can regulators, societal stakeholder and standards developers react effectively to new AI harms that emerged quickly?
- How can regulators, societal stakeholder and standards developers collaborate to determine the correct acceptable application-appropriate thresholds for technical assessment of AI risks, e.g. voice recognition bias tests in education vs. emergency dispatch applications?

11:45 – ENFORCEMENT OF DATA PROTECTION BY DESIGN & BY DEFAULT: CONSEQUENCES FOR THE UPTAKE OF PRIVACY-ENHANCING TECHNOLOGIES IN THE EU

Academic ☆ **Business** ☆☆ **Policy** ☆☆☆
Organised by Future of Privacy Forum (FPF) (BE)
Moderator Christina Michelakaki, Future of Privacy Forum (FPF) (BE)
Speakers Marit Hansen, State Data Protection Commissioner of Land Schleswig-Holstein (DE); Jaap-Henk Hoepman, Radboud University Nijmegen/University of Groningen (NL); Stefano Leucci, European Data Protection Supervisor (EDPS) (BE); Cameron Russell, eBay (IE)

Data Protection Authorities (DPAs) across the EU have been strictly enforcing the GDPR's Article 25 rules on Data Protection by Design & by Default (DPbD&bD), with orders and penalties in most EU countries. On the other hand, organizations across the EU are increasingly relying on technical measures to protect their stakeholders' personal data. This panel will explore DPbD&bD enforcement precedents, as well as their relationship with data integrity and confidentiality principles as they relate to the adoption of Privacy-Enhancing Technologies (PETs). Corrective actions from regulators may illustrate scenarios in which implementing specific PETs is appropriate to comply with GDPR requirements. However, further clarity may be needed in the form of explicit guidance from the European Data Protection Board (EDPB) and alignment with policymakers and watchdogs in other jurisdictions.

- How are DPAs applying Article 25 GDPR when it comes to the adoption of technical measures by data controllers and processors?
- What are the most mentioned PETs in DPAs' enforcement record?
- Are there under-explored technical solutions in corrective actions in Europe?
- Could clear guidance from EU regulators generate confidence for wide-ranging adoption of PETs in different countries, sectors and settings?

13:00 - LUNCH

14:15 – PREPARING CRYPTOGRAPHY FOR THE QUANTUM AGE

Academic ☆☆ **Business** ☆ **Policy** ☆☆☆
Organised by Quantum Software Consortium (NL)
Moderator Laima Jančiūtė, University of Amsterdam (NL)
Speakers Tanja Lange, Technical University Eindhoven (NL); Melissa Rossi, French cybersecurity agency (ANSSI) (FR); Ot van Daalen, University of Amsterdam (NL); Bas Westerbaan, CloudFlare (NL)

Quantum computing promises to break public key encryption. If you'd have access to a quantum computer, you would be able to decipher intercepted messages. These computers are not yet powerful enough, but when they are, this has significant implications for privacy and data protection. And experts estimate that such a computer will be probably developed in 10-15 years. The question is: what should governments and organisations do to prepare for this, and what laws must there be to safeguard against abuse of these powerful machines?

- What are the risks of quantum computing to public key encryption?
- What obligations do governments have to facilitate the transition to quantum-resistant cryptography?
- What are the obligations of governments with regard to the use of quantum computers for decryption?
- What practical obstacles are there for transitioning to quantum-resistant cryptography?

15:30 - COFFEE BREAK

16:00 – EDPL YOUNG SCHOLAR AWARD

Academic ☆☆☆☆ **Policy** ☆☆
Organised by Lexxion Publisher (DE)
Moderators Franziska Boehm, Karlsruhe Institute of Technology (DE), Bart van der Sloot, Tilburg University (NL)
Speakers Magdalena Brewczyńska, Tilburg University (NL); Mona Winau, Karlsruhe Institute of Technology (DE); Benny Rolle, University of Goettingen (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.

- Magdalena Brewczyńska, Tilburg University (NL) - From 'legitimacy' in EU primary ław to the principle of 'lawfulness' in the secondary data protection legislation and back to 'legitimacy': In search of rationality and consistency
- Mona Winau, Karlsruhe Institute of Technology (DE) - Areas of tension in the application of AI and data protection law
- Benny Rolle, University of Goettingen (DE) - Fair data protection damages: Tension between troublemakers, legal techs and real harm

The papers will be discussed by the jury made up of EDPL Board Members Indra Spiecker gen. Döhmann, Goethe-Universität Frankfurt (DE), Franziska Boehm, Karlsruhe Institute of Technology (DE), Maria Tzanou, University of Sheffield, (UK), and Orla Lynskey, London School of

Economics (UK).

At the end of the panel, the winner of the 7th EDPL Young Scholar Award will be announced.

17:15 – GDPR AUTOMATION: MIGHT THE LAW (UNINTENTIONALLY) PUSH TOWARDS AUTOMATION?

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by LSTS, Vrije Universiteit Brussel (VUB) (BE)
Moderator Desara Dushi, LSTS, VUB (BE)
Speakers Thomas Zerdick, European Data Protection Supervisor (EU); Aurelia Tamò-Larrieux, Maastricht University (NL); Asia Biega, Max Planck Institute for Security and Privacy (MPI-SP) (DE); Gianmarco Gori, LSTS, Vrije Universiteit Brussel (BE); Mikołaj Otmianowski, DAPR (PL)

With the adoption of the GDPR, data subjects gained more power in tracking their data, while for entities processing personal data that means higher responsibilities and burden, particularly because demonstrating compliance with GDPR principles is not that easy. A solution that is gaining popularity, is the use of certain legal technologies which claim to offer automation of GDPR compliance. But their use comes with certain costs. Discussion in this panel will revolve around issues of GDPR automation, whether certain GDPR provisions lend themselves to automation, and whether automation actually contributes to GDPR compliance. The panel follows the form of a debate, to allow for a better exchange of views from the panelists composed of different stakeholders.

- Do particular provisions of the GDPR push towards automation?
- Does automation actually contribute to GDPR compliance? If yes, to what extent? What problems does automation solve and what new problems does it cause?
- Who would be held liable if things go wrong in an automated GDPR compliance situation (the developer, the controller, the processor, or all of them)? Under what conditions?
- Is automation a form of or a means for GDPR compliance? What normative implications arise when automating GDPR compliance?

18:30 – COCKTAIL SPONSORED BY UBER

in Le Village

CPDP2023 WORKSHOPS AT M-VILLAGE GRANDE

08:45 – Workshop DATA AUTONOMY IN HIGHER EDUCATION: THE QUEST FOR 'PUBLIC VALUES IN THE CLOUD'

Organised by University of Groningen (NL)
Workshop facilitator Ronald Stolk, CIO, University of Groningen (NL)
Speakers Frank Karlitschek, Nextcloud (NL); Mando Rachovitsa, University of Groningen (NL); Magdalena Rzaca, GÉANT & IPR Legal Advisor (NL); Oskar J. Gstrein, University of Groningen (NL)

Public institutions are increasingly dependent on international data flows, cloud-based commercial applications, and remote data storage. While these infrastructures promise efficiency, the power of public institutions to make decisions about 'their data' disappears. This raises data protection concerns and — potentially more importantly — undermines 'data autonomy'. In this panel we explore this tension from the perspective of public universities, which are particularly interesting: On the one hand, they are based on the promotion of public values. Universities require 'academic freedom' and independence to flourish. They develop Open-Source applications for teaching and research. On the other hand, they are required to use funds efficiently, and provide state-of-the-art working and research environments for students, researchers, and staff. But what should higher education do to address the increasing dependence on 'Big Tech' with commercial objectives, while safeguarding data autonomy and public values?

- What are the threats to academic freedom and data protection in times of cloud-based data handling and remote teaching?
- Which strategies do universities have to navigate the intersection between dependency on Big Tech and promoting less-popular Open-Source initiatives?
- How to respect public values while using commercial applications?
- Can current regulatory frameworks deliver enough, appropriate, and desirable guidance?

10:00 - COFFEE BREAK

10:30 – Workshop GDPR CERTIFICATION IN PRACTICE

Organised by Mandat International (INT)
Speakers Sébastien Ziegler, Mandat International (CH); Alain Herrmann, Commission Nationale pour la Protection des Données (CNPD) (FR); Emanuele Riva, ACCREDIA (IT); Luca Bolognini. Istituto Italiano per la Privacy e la Valorizzazione dei Dati (IT)

Recently, EDPB adopted Europrivacy as European Data Protection Seal under Art. 42 GDPR. This session will present the latest developments related to GDPR certification and accreditations. The session will also highlight the various use of Europrivacy criteria, for instance to document compliance and reduce risks, as well as the impact of GDPR certification to value compliance. The session will cover key questions such as: How to support a smooth transition from compliance to certification? What is the added value of a certification under Art. 42 GDPR? How can certification reduce the risks for data subjects, data controllers and processors? Can certification facilitate international data transfer? What are the characteristics and advantages of certification compared to other mechanisms, such as codes of conduct, standard contractual clauses, and corporate binding rules?

11:45 – Roundtable "IT'S NOT ABOUT THE PERSONAL DATA, STUPID! IS IT TIME TO FOCUS LEGAL PROTECTION AGAINST RISKS OF THE DIGITAL SOCIETY ON SOMETHING ELSE?"

Organised by ERC INFO-LEG project, Utrecht University (NL)
Moderator Nadya Purtova, Utrecht University (NL) & Raphaël Gellert, Radboud University (NL)
Speakers Hielke Hijmans, Belgian DPA (BE); Laurence Diver, VUB (BE); Michael Veale, UCL (UK)

"Personal data" has not performed well as a trigger of legal protection against risks of the information society. Its broad interpretation in theory makes the GDPR "the law of everything" digital. Yet, in practice, many information practices fall through the GDPR cracks: controllers construe "personal data" narrowly and do not apply the GDPR where they should; PETs obfuscate the boundary between identifiable and anonymous; the GDPR is not designed to tackle group information harms.

Experts from the law practice and academia will discuss if the regulatory focus on personal data as a trigger of legal protection obscures the problems we want to solve, and if focusing on different regulatory targets will do the job better. If it's time for a redesign of the legal protection against harms of the digital society, how should it look like?

- Are all the risks of the digital society that the GDPR aims to address contingent on a certain type of information processed, specifically, "personal data", or do some of the problems materialise regardless of the meaning of information used?
- Should the broad scope of personal data be narrowed down and problematic digital practices (automated decision-making, algorithmic discrimination, or platform exploitation) be regulated instead? What would those practices be?
- Should design and use of software with impact on people be regulated among those practices?
- Could the general principles of data protection serve as a blueprint for the general principles of design and use of algorithms? What added value would this approach have compared to the AI Act?
- Will a narrower scope of the GDPR in combination with the general principles of design and use of software make a positive difference in terms of compliance, enforcement and quality of legal protection compared to the status quo?

13:00 - LUNCH

,14:15 – Workshop STATE-OF-PLAY OF PRIVACY-PRESERVING MACHINE LEARNING (PPML) - AUDITING BIAS, MITIGATING PRIVACY RISKS IN ML-SYSTEMS

Organised by Future of Privacy Forum (BE)
Workshop facilitator Rob van Eijk, Future of Privacy Forum/FPF Europe (NL)
Speakers Lindsay Carignan (BR); Adriano Koshiyama (US); Victor Ruehle (DE); Reza Shokri (SG)

Join FPF for a workshop at CPDP 2023 on the state-of-play of Privacy-Preserving Machine Learning (PPML). In this workshop, we aim to contribute to clearing the path to alternative solutions for processing (personal) data with Machine Learning. Attendees will learn about Auditing bias in machine learning systems (Topic 1) and Mitigating and Auditing Privacy risks in Machine Learning (Topic 2). We will survey some methods and approaches to auditing bias in algorithmic systems. We will discuss the interaction of bias in machine learning systems and regulations such as the EU AI Act. We will use a practical example of the NYC bias audit law problems and approaches in assessing and protecting personal data. Furthermore, we will introduce privacy auditing to measure the privacy risk in ML systems quantitatively. We will demonstrate how this framework can be used to compare the effectiveness of anonymisation and pseudonymisation techniques such as k-anonymization, (personal) data scrubbing, and Differential Privacy to achieve the best, scenario-dependent, privacy/utility trade-off.

15:30 - COFFEE BREAK

16:00 – Workshop FUTURE TREND: THE CONFLICT BETWEEN CYBERSECURITY AND PRIVACY

Organised by Deloitte (BE)
Workshop facilitator Justin Norman (Deloitte, BE)
Speakers Arthur Testa, Deloitte (BE); Tim Bielders, Deloitte (BE); Justin Norman, Deloitte (BE)

A focus on the conflict between cybersecurity and privacy. There are various privacy concerns regarding new AI cybersecurity technologies and growing popularity of Zero Trust design principles. These technologies and cybersecurity framework collect more personal data and monitor data subjects and their actions across the network. While Recital 49 of the GDPR explains that the protection of personal data stored within an information network constitutes as an overriding legitimate interest, the personal data processed for these purposes must still be strictly necessary and proportionate. It is difficult for organisations to know what measures can be taken to improve cybersecurity and still comply with the GDPR principles. These concerns will only continue to grow as AI technologies will also be harnessed by malicious actors, allowing them to develop more sophisticated malware. In turn, requiring organisations to adopt more intrusive cybersecurity technologies.

- Introduction to AI cybersecurity technologies and ZeroTrust
- Overview of guidance and statements from supervising authorities regarding cybersecurity and regulatory obligations regarding privacy, data protection and cyber security

- Overview of the current trends related to cybersecurity attacks
- How should organisations deal with this cyber security changes in light of privacy concerns
- Future trends, what to expect in the next couple years regarding new threats, cybersecurity and privacy

17:15 – Workshop THE STATE OF DATA PROTECTION LAW ACADEMIA

Organised by Data Protection Law Scholars' Network (DPSN)
Workshop facilitator Gloria Gonzalez Fuster, VUB (BE)

A plethora of substantive issues related to data protection law is touched upon yearly during the CPDP Conference. In line with our goals of supporting exchange between scholars, advancing the bridges between data scholarship of continents, and promoting diversity, this session invites the large and diverse group of data scholars that CPDP brings together to take stock of the state of data protection law academia. Attendees of this session will be encouraged to discuss topics that are considered the most pressuring to be addressed by the DPSN community in an interactive setting to understand the underlying reasons and possible solutions. Like in all DPSN events, there will also be an element of networking in which we encourage attendees to get to know each other.

18:30 – COCKTAIL SPONSORED BY UBER

in Le Village

CPDP2023 WORKSHOPS AT M-VILLAGE MIDI

08:45 – WORKING & MEETING SPACE

10:00 - COFFEE BREAK

10:30 – Workshop PRIVACY THREAT MODELING FOR AI SYSTEMS

Organised by Rhite (NL)
Workshop facilitator Isabel Barberá, Rhite (NL)

Do you want to learn how to identify risks when developing AI systems?

In this hands-on workshop you will experience how an AI threat modeling session works using the open-source AI risk assessment tool PLOT4ai (https://plot4.ai).

PLOT4ai stands for Privacy Library of Threats for Artificial Intelligence. It is a threat modeling methodology inspired by LINDDUN and created to help build Responsible AI systems. It contains 86 AI threats classified in 8 categories: Technique & Processes, Accessibility, Identifiability & Linkability, Unawareness, Non-compliance, Ethics & Human Rights, Safety and Security.

After a short introduction to privacy threat modeling and PLOT4ai, you will practice in groups how to threat model an AI system during the design phase by working on a use case. We will do this using the physical card game from PLOT4ai.

11:45 – Workshop INCLUSIVE CO-DESIGN AND SOCIETAL ACCEPTANCE OF EMERGING SECURITY TECHNOLOGIES: AMBITIONS AND BEST PRACTICE

Organised by DARLENE (Deep AR Law Enforcement Ecosystem) by Centre for IT & IP Law, KU Leuven / CiTiP (BE)
Workshop facilitator Isabela Maria, Rosal, Centre for IT & IP Law, KULeuven/CiTiP (BE)
Speakers Thomas Marquenie, Centre for IT & IP Law, KU Leuven/CiTip (BE); Fabienne Ufert, Trilateral Research LTD, TRI (IE); Evaldas Visockas, Lithuanian Police, PL (LT); Michael Friedewald, Fraunhofer-Gesellschaft (DE)

New security technologies (including AI) are intended to promote public safety, security and increase societal resilience. At the same time, security technologies spur controversies and can have enormous societal, ethical and legal impact. This presentation features legal, ethics, and policy experts, as well as a law enforcement agency representative, who will share experiences on how to build an inclusive digital society, considering the role of integrated ethical, legal and societal impact assessments and an interdisciplinary co-design approach for developing and deploying new security technologies. For that, two main case studies will be presented: the H2020 project DARLENE and HorizonEurope project TRANSCEND (also potentially drawing from H2020 SPARTA). The presentation will focus on methods and results of meaningful citizen and end-user engagement to ensure that end-users, citizens and society as a whole can accept and effectively use cutting-edge security solutions.

- What do impact assessment and co-design mean for new security technologies and why are they important?
- What are useful methodologies for meaningful citizen engagement in the development of new security technologies for law enforcement and other first response cases
- What are the ambitions, main results and lessons learned from the societal engagement activities in DARLENE and TRANSCEND?
- How can we reconcile end-user needs and views regarding new security technologies with corresponding societal needs and concerns?

13:00 - LUNCH

14:15 – WORKING & MEETING SPACE

15:30 - COFFEE BREAK

16:00 – Workshop THE UK'S APPROACH TO INTERNATIONAL DATA TRANSFERS: HOW TO BUILD TRUST, DELIVER GROWTH AND FIRE UP INNOVATION

Organised by Department for Science, Innovation and Technology (UK)
Workshop facilitator Siddharth Bannerjee, BCMS (UK)

This session will cover the key opportunities and challenges arising from the UK's involvement in the international data transfers space, and the legislative, policy and regulatory responses to these. Highlights include:

- Lessons learned from the Parliamentary passage of the Data Protection and Digital Information Bill.
- Insights from engagement with the Global Cross-Border Privacy Rules (CBPR) forum.
- Reflections on the work of the International Data Transfers Expert Council on: Multilateral solutions for scalable international data flows; Building global consensus on trusted government access to data; UK government tactics and strategy for achieving its international goals; The value and importance of data flows: case studies and evidence

17:15 – Workshop MOOT COURT: THE VALUE OF HEALTH DATA

Organised by Department of Innovation and Digitalisation in Law, University Vienna (AT)
Workshop facilitator Theresa Henne, Department of Innovation and Digitalisation in Law, University Vienna (AT)
Speakers María José Alarte Aceñero, Quibim (ES); Aline Blankertz, Wikimedia Germany (DE); Daniele Regge, University of Torino & Radiology Unit, Candiolo Cancer Institute, Torino Italy (IT); Lorraine Maisnier-Boché, McDermott, Will & Emery & Paris II and Paris V Universities (FR)

In this fictional Court case, we will discuss how data providers should be rewarded for their contribution to the development of medical AI applications. Workshop participants will support one of the parties in finding the most convincing arguments in order to win the case.In this scenario, the European Health Data SpaceRegulation (EDHS) entered into force, obliging data holders to make data available for the development of health care applications against a "reasonable fee". A Belgian technology company has developed an AI-driven cancer diagnosis tool based on data accessed via the EDHS and provided by a data altruism organisation.The AI application was recently sold to a US company for 30 million EUR. The sale of the AI application is challenged in Court by a clinical data provider and a patient representative group raising the following questions.

- The clinic provided a 1/3 of the total data set used to develop the AI application. As a compensation for the clinic's cost for providing and enriching the data, it received the sum of 10,000 EUR. The clinic challenges the original agreement arguing that considering the profit the AI company made, the meaning of a "reasonable fee" must be renegotiated. They claim it must include not only compensation for their costs but also a share of the profit generated by the AI innovation.
- The AI application was developed based on data provided by the data altruism organisation AI4HEALTH.The non-profit collects data from patients based on their consent and grants access to third parties for uses in the public interest. The patient representative group challenges whether the Belgian AI company used the data in the public interest. Since the AI application was sold to a US company, they fear that patients in the EU will not directly benefit from the cancer diagnosis tool.

18:30 – COCKTAIL SPONSORED BY UBER

in Le Village

FRIDAY 26TH MAY 2023

Please note that this is a preliminary version of the programme.

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

CPDP2023 PANELS AT GRANDE HALLE

08:45 – SEE YOU IN COURT!

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by NOYB (AT)
Moderator Romain Robert, NOYB (AT)
Speakers Augusta Maciuleviciute, BEUC (BE); Jurjen Lemstra, Lemstra Van der Korst (NL); Stefaan Voeat, Leuven University (BE); Petra Leupold, VKI (AT)

In parallel to the enforcement of their digital rights (GDPR, DMA, DSA, ePrivacy, and so on) by public authorities, users can also turn to the judges to enforce their rights. Access to justice is however not always guaranteed. The Directive on Collective Redress (RAD) was aimed at being implemented by the end of 2022 by Member States and will enable consumers to bring collective actions to enforce their rights. The panel will discuss how the Directive could be a game changer for the collective enforcement of users' rights and under which conditions. Speakers will also see how the existing national regimes can address -or not- the challenges of access to justice and collective enforcement of digital rights.

- What are collective actions in the EU?
- What can we expect from collective actions?
- How can collective redress actions be financed?
- Are we ready to see you in court?

10:00 - COFFEE BREAK

10:30 – FAIRNESS IN PERSONALISATION: THE ROLE OF TRANSPARENCY, USER CONTROL, AND THE BALANCE BETWEEN FUNDAMENTAL RIGHTS

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by Meta (IE)
Moderator Maximilian, Von Grafenstein, UdK Berlin/Alexander von Humboldt Institute for Internet and Society (DE)
Speakers Cecilia Alvarez, Meta (ES); Christiane Wendehorst, European Law Institute (AT); Giovanni De Gregorio, Bocconi University (IT); Vera Jungkind, Hengeller Muller (DE)

Fairness is required under the GDPR, but little guidance has been provided on how to implement it in practice. How should fairness in privacy and data protection be placed in the right context, and be balanced against other fundamental rights—such as the freedom of expression, the freedom to conduct a business, and the right to integrity? Why is it important to keep other rights in mind when interpreting GDPR, for instance, those concerning business models and international data transfers? And what role do other areas of law, namely contract law, play? This panel will address how fairness in advertising is related to the right implementation of the privacy-by-design principle. The speakers will also explore the role of user-centric tools for transparency and controls that are designed for people, businesses, and society to have a fair advertising experience.

11:45 – THE COLLECTION, SHARING, AND USE OF GENDER DATA

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by Northeastern University (US)
Moderator Nasser Eledrooos, Northeastern Law's Center for Law, Information and Creativity (CLIC) (US)
Speakers Kevin Guyan, University of Glasgow (UK); Os Keyes, University of Washington (US); Ari Ezra Waldman, Northeastern University (US)

Automated decision-making systems use sex and gender data in complex algorithmic systems that purport to predict population level outcomes. This poses a data dilemma, particular for transgender, nonbinary, and gender-nonconforming individuals. On the one hand, more and better collection, sharing, and use of data about marginalised populations can highlight discrimination, improve access to health care, and respect the dignity of all persons. On the other hand, legibility comes with risks, and there is virtue in the state and data-extractive companies knowing less about people stigmatised in society. This panel will address the law and policy implications of gender and sexual orientation data collection, sharing, and use in US, European, and global jurisdictions, considering in particular how law can, if at all, navigate this data dilemma.

- Should the state be in the business of collecting, sharing, and using gender data at all?
- What standard, if any, should govern the collection, sharing, and use of gender data?
- Should the same rules apply to private companies and governments?
- What strategies, perhaps outside the law, are necessary for building an equitable system of sexual orientation and gender data collection?

13:00 - LUNCH

14:15 – SUBJECTS AND STRUCTURES: RE-IMAGINING DATA PROTECTION AS A CRITIQUE OF POWER

Academic ☆☆☆ **Business** ☆ **Policy** ☆☆
Organised by Fraunhofer ISI (DE)
Moderator Michael Veale, UCL (UK)
Speakers Aisha Kadiri, École Normale Supérieure (FR); Victoria Guijarro Santos, University of Muenster (DE); Chloé Berthélémy, EDRi (BE); Felix Bieker, Office of the Data Protection Commissioner of Schleswig-Holstein (ULD) (DE)

Our panel proposes new perspectives on data protection, taking the paradigmatic GDPR as a starting point, yet moving beyond its provisions. To find a hopeful future for data protection, we look at its past, non-individualistic perspectives on the law and non-Western practices of the present. The panel will lay out how to expand our understanding of data protection to counter current harmful data practices. These practices include the concentration of informational power in the hands of a few, the exploitation of data subjects and the domination of socially marginalized persons. We will further consider the socio-economic legal and informal structures that enable such practices and outcomes and focus on the following questions:

- How is the data subject formed by and navigates through structures of power and competing informational norms?
- How should data-based discrimination be governed?
- How do data laws distribute power?
- How can we protect communities and society as a whole from adverse effects of data practices?

15:30 - COFFEE BREAK

16:00 – A SAFE SPACE TO CREATE - HOW PLATFORMS ARE APPROACHING MINORS' PRIVACY

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by TikTok (US)
Moderator Natascha Gerlach, CIPL (BE)
Speakers Caroline Goulding, TikTok (IE); Simone Vibert, Internet Matters (UK); Darragh McCashin, Irish Observatory on Cyberbullying, Cyberhate and Online Harassment / School of Psychology, Dublin City University (IE)

While minor data privacy protection policies and regulations may vary across regions, there's no disagreement among platforms that younger people should be top of mind when thinking about how to design age-appropriate privacy settings, controls and experiences. Platforms should also design with regulatory requirements in mind. From the General Data Protection Regulation (GDPR) in the EU and the Age Appropriate Design Code (Children's Code) in the UK, to the Children's Online Privacy Protection Act (COPPA) and a host of upcoming new state laws in the U.S., protecting young people's privacy is best accomplished as a collaborative effort between regulators and platforms.

This panel will explore how platforms should think about designing for younger people to ensure they have a safe space to creatively express themselves while meeting privacy, safety and regulatory requirements.

- How to build with age-appropriate design in mind?
- What challenges persist in safeguarding younger people's privacy across the industry?
- Are there elements of recent key regulations companies should focus on when creating a minor-specific privacy policy?
- How platforms should think about collaborating with regulators, industry peers and other organisations.

17:15 – THE END OF ONLINE BEHAVIOURAL ADVERTISING

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by eLaw - Center for Law and Digital Technologies Leiden University (NL)
Moderator Lex Zard, eLaw Leiden University (NL)
Speakers Mireille Hildebrandt, Vrije Universiteit Brussel (BE); Paul Nemitz, European Commission (EU); Sandra Wachter, University of Oxford (UK); Marco Blocher, NOYB (AT); Wojciech Wieworoski, EDPS (EU)

Online behavioral advertising (OBA) is the main revenue stream of ad-based internet. It is claimed to be the root of many online harms (e.g., privacy, autonomy, consumer and social welfare, democracy, and human rights). While GDPR regulates OBA, some scholars claim that OBA's harms escape its grasp. Nevertheless, recent developments in enforcing the GDPR reveal that it is challenging for the industry to continue the practice. For example, in one case, CJEU considers the legitimacy of the consent framework that operationalizes OBA's programmatic auction; in another, it considers the legitimacy of personalizing advertisements as a contractual necessity. In addition, consumer protection authorities increasingly apply UCDP to practices that operationalize OBA. Lastly, DSA prohibited using OBA to target minors and when relying on special data categories. Nevertheless, as in Case C 184/20, CJEU expanded the pool of such data; the question is to what extent is OBA legitimate in the EU?

- Online behavioral advertising
- Safeguarding human dignity
- Monetisation of online environment
- Digital constitutionalism in the EU

18:30 – CLOSING REMARKS BY WOJCIECH WIEWIOROWSKI (EPDS) AND CHRISTOPHER KUNER (VUB)

19:00 – COCKTAIL SPONSORED BY PRIVACY SALON

in Le Village

08:45 – BEYOND ETHICS WASHING: IMPACT ASSESSMENTS, AUDITS, AND OVERSIGHT FOR AI

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

Organised by Helsinki Institute for Social Science and Humanities, University of Helsinki (FI)
Moderator Mirko Tobias Schäfer, Utrecht University/University of Helsinki (NL/FI)
Speakers Paul Nemitz, European Commission (EU); Iris Muis, Utrecht University Data School (NL); David Graus, Randstad (NL); Maria Koomen, Open Governance Network for Europe (BE)

A plethora of ethics manifestos, guidelines and frameworks calls for responsible AI and data practices. Legislation is under way to regulate AI practices. But how to effectively close the gap towards practical application? How can organisations implement practices that stimulate responsible application of AI systems, and how can -increasingly digitized- democratic societies establish necessary checks and balances? Looking further than the good intentions of ethics guidelines, this panel discusses which best practices are most effective to align the design and use of AI systems with the values of our open and democratic societies. This panel investigates how practical approaches, such as impact assessments and audits, and the role of oversight bodies help to establish responsible and safe uses of AI and big data practices and can constitute accountability.

- Should impact assessments be mandatory?
- Who is responsible for oversight and enforcement?
- Can we hold algorithms accountable?
- What are the limits to good governance of AI?

10:00 - COFFEE BREAK

10:30 – WHOSE DIGITAL FUTURE? ENGAGING CITIZENS IN AI DEVELOPMENT AND IMPACT ASSESSMENT

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

Organised by European Center for Not-for-Profit Law (ECNL) (NL)
Moderator Berna Keskindemir, ECNL (NL)
Speakers Mirko Tobias Schäfer, Utrecht University (NL); Alyna Smith, PICUM (BE); Laura Galindo, Meta (DE); Jana Gajdosova, EU Fundamental Rights Agency (EU)

This session explores opportunities for companies and policymakers to meaningfully engage external stakeholders in tech policy and development, a cornerstone of norm creation. Yet this is challenging in practice, from limited decision-making power of civil society to short product development timelines. Using AI governance as a case study, speakers will share their practical experiences related to stakeholder engagement when developing, deploying, and regulating AI. Drawing on a novel method for participation in AI governance developed by the European Center for Not-for-Profit Law, with input from 130+ experts, speakers will contextualise multistakeholder engagement within the European tech policy ecosystem. From data protection standards to the EU AI Act and a future Council of Europe Convention on AI, the session aims to ensure a regulatory environment for a truly inclusive digital society, especially for marginalised and vulnerable groups.

- How to ensure meaningful, and not performative, participation of civil society organisations and people when developing and using AI systems?
- How can the EU AI Act or other policy instruments contribute to more inclusive development of technology?
- What is the value of consulting people and communities affected by AI?
- What are the obstacles, for civil society organisations and people on the one hand and AI developers on the other?

11:45 – HAVE YOU TRIED ASKING? ENGAGING WITH CITIZENS IN POLICY AND PRODUCT DEVELOPMENT

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

Organised by Information Commissioner's Office (ICO) (UK)
Moderator Clara Clark Nevola, ICO (UK)
Speakers Marie Potel-Saville, Amurabi (FR); Emma Cantera, Organisation for Economic Co-operation and Development (OECD) (INT); Anja Dinhopl, Google (DE)

This panel aims to showcase and discuss the importance of listening to user and citizen perspectives and the key role this plays in achieving privacy by design and transparency. It will explore approaches to engaging with members of the public when designing for privacy. The panellists' views will be sought on how to successfully incorporate deliberative design, citizens' consultations or other public engagement strategies into the development of privacy-focused products, services or policies. The panel will consider whether and how data protection can be strengthened by consulting with individuals during the development of both policy or products and services.

- How should we engage citizens in data protection discussions?
- What are the risks or limitations of involving citizens in policy making or product development?
- What do citizens' perspectives add to policy making and/or product development?
- Who are these "citizens"? How to recruit/select groups to engage with?

13:00 - LUNCH

14:15 – THE SOCIAL AND ETHICAL IMPLICATIONS OF IMPLANTABLE ENHANCEMENT TECHNOLOGY

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

Organised by Centre for Business Information Ethics, Meiji University (JP)
Moderator Andrew A. Adams, Centre for Business Information Ethics, Meiji University (JP)
Speakers Stephanie Gautier, Grenoble Ecole de Management. (FR); Yohko Orito, Ehime University (JP); Mario Arias Oliva, Complutense University of Madrid (ES); Richard Benjamins, Telefonica (ES)

Most implantable technology approved for human use currently is therapeutic or designed to provide the user with minimal, or at best average, capabilities compared to organic functionality. However, there is a great deal of technical research into implantables which would enhance capabilities beyond human norms, or even beyond human limitations, as well as a community which actively desires to have such technology implanted. Based on interviews with experts in France, Spain and Japan, the panel will provide an overview of the social, legal and ethical concerns (such as privacy, security, autonomy and inequality) about whether such technologies should be allowed and if so under what kinds of regulatory systems. Physical and mental augmentation technologies as well as the impact of national culture on attitudes will be covered.

- What physical and intellectual enhancements are likely possible from implantable technology in the next thirty years?
- Should research (including human trials) into enhancement implantables be permitted?
- What social, legal and ethical issues arise from the potential availability of enhancement implantables?
- How should implantable enhancement technologies be regulated?

15:30 - COFFEE BREAK

16:00 – THE CHANGING FACE OF CONSUMER PROTECTION IN AFRICA'S DIGITAL ECONOMY

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

Organised by Lawyers Hub (KE)
Moderator Risper Onyango, Lawyers Hub (KE)
Speakers Linda Bonyo, Lawyers Hub (KE); Vellah Kedogo Kigwiru, Technical University of Munich (DE); Jorge Clarke, International Research Center on Artificial Intelligence (FR); Ken Agengo, Ndoa Wedding Films (Business and Startups) (KE)

E-commerce has evolved since its inception in the late 1990s, putting consumers on centre stage. Increased digital commerce has meant that consumers have convenience and near instant access to online goods and services, however dangers lurk on fulfilment. The line between businesses and consumers continues to blur due to the increased financial opportunities opened to consumers to sell, rent, and perform tasks for other consumers through Internet platforms. This rampant online activity also generates a wealth of data used to sketch and ruminate consumer profiles which have become core to ecommerce business models but also brings risks, including privacy and security risks. Inversely, of 54 African countries, only 25 have laws on online consumer rights and electronic transactions (4 have draft laws) while just over half of the countries have data protection laws; a majority lacking the needed enforcement mechanisms.

- What are the emerging issues in consumer protection in the digital economy and what categories of persons/consumers are most vulnerable?
- How does consumer protection in this era intersect with other emerging issues such as data protection, cybersecurity and technologies such as artificial intelligence?
- To what extent have existing consumer protection regulations addressed the issue of inclusivity and standards for digital products and platforms?
- How can policy and regulatory frameworks be leveraged to create a well-functioning digital economy?

17:15 – GDPR & LGPD: EXPLORING THE POTENTIAL OF CODES OF CONDUCT ACROSS BORDERS

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

Organised by SCOPE Europe (EU)
Moderator Frank Ingenrieth, SCOPE Europe (EU)
Speakers Natasha Torres Gil Nunes, Conexis Brasil Digital, Brazilian National Data Protection Authority (ANPD) (BR); Nathaly Rey, Google Cloud (ES); Ricardo Campos, Goethe Universität Frankfurt am Main, Instituto LGPD, Data Protection Commission at the Federal Council of the Brazilian National Bar Association (DE); Corinna Schulze, SAP (EU)

This panel seeks to explore the global potential of co-regulatory tools in the field of data protection. Panellists will discuss the benefits of implementing codes of conduct to harmonise and build trust amidst the complexity of today's digital economy. In this spirit, this group of experts will share the challenges of implementing the LGPD on the Brazilian side, while providing insights on the successful experience of the European cloud sector with co-regulation. Through an interactive and dynamic session, the audience will be able to understand how European and Brazilian key stakeholders are collaborating across borders to further develop robust and innovative data protection standards.

- What are the parallels and differences between the Brazilian LGPD and the European GDPR?
- How to increase cross-sectoral and cross-border cohesion in the establishment of robust data protection standards?
- What is the European privacy sector's experience with implementing codes of conduct as a GDPR compliance tool?
- What are the limitations of currently implemented compliance mechanisms and how can stakeholders jointly optimise these instruments?

18:30 – CLOSING REMARKS BY WOJCIECH WIEWIOROWSKI (EPDS) AND CHRISTOPHER KUNER (VUB)

in Grande Halle

19:00 – COCKTAIL SPONSORED BY PRIVACY SALON

in Le Village

FRIDAY 26 MAY 2023

08:45 – DARK PATTERNS: DEFINITIONS AND EVIDENCE FOR REGULATORS

Academic ☆☆ **Business** ☆ **Policy** ☆☆☆
Organised by Inria (FR)
Moderator Nataliia Bielova, Inria (FR)
Speakers Colin M. Gray, Purdue University (US); Laura Litvine, Behavioural Insights Team (FR); Bertrand Pailhes, CNIL (FR); Dries Cuijpers, Autoriteit Consument & Markt (NL)

Online services such as websites, social media, mobile and IoT apps provide user interfaces proposing to control its users' personal data. While Data Protection and Consumer law set high-level principles applicable to such interfaces, online service providers still have a large design space to test various interfaces on its users. This situation gave rise to the use of manipulative tactics in UX/UI commonly known as dark patterns, or deceptive design. Today, policy makers and regulators worldwide are concerned. First, dark patterns are difficult to define -- the line between nudging techniques that may be perceived as acceptable marketing strategies and intentional deception causing detriment to users is often blurred. Second, it is unclear what is acceptable evidence for regulators to demonstrate presence of dark patterns to sustain their legal proceedings. This panel aims to discuss the unified definitions of dark patterns and analyze which evidence can be legally relevant for regulators to protect data subjects from such manipulative practices.

- How do existing and upcoming Data Protection and Consumer laws regulate the presence of dark patterns?
- Are there unified and acceptable definitions of dark patterns for policy makers and regulators?
- What kind of evidence of dark patterns has been so far acceptable for policy makers and regulators?
- Which empirical research insights can be useful to gather evidence of dark patterns?

10:00 - COFFEE BREAK

10:30 – INCREASED GOVERNMENT ACCESS TO PERSONAL DATA: RETHINKING THE ROLES OF CITIZENS AND THE PRIVATE SECTOR

Academic ☆☆☆ **Business** ☆ **Policy** ☆☆
Organised by Academia Sinica (TW)
Moderator Tyng-Ruey Chuang, Academia Sinica (TW)
Speakers Wen-Ting Yang, Maastricht University (NL); Ming-Syuan Ho, Academia Sinica (TW); Mélanie Dulong de Rosnay, Center for Internet and Society, CNRS (FR)

The datafication of the public sector appears to be a global trend. Related topics such as e-government or digital governance have received much attention. Many countries are shaping their data policies to increase data exchange in the public sector and to gain access to privately held data, as can be seen in their national data strategies. New EU-level legislation has also been issued, aiming to facilitate open data development and proper data governance. Disturbing measures for contact tracing and data collection, however, proliferate over the past few years in the name of fighting the COVID-19 pandemic even though public health and data protection policies vary across countries. We believe there is an urgent need to re-examine the relationship between citizens, the private sector,and the public sector in particular with regard to personal data access and reuse.

- What are the legal, social, and other tensions caused by the existing data use practices of governmental departments and agencies?
- How do awareness, norms, resources, technologies, and tools impact on people's participation in forming consensus about the access to and reuse of their personal data?
- To what extent has the public changed their view on personal data protection after COVID? How and why have they changed?
- What are the regional differences and characteristics in the practice of personal data protection?

11:45 – THE NEW E-EVIDENCE REGULATION: PROBLEM SOLVED OR OPENING OF A PANDORA'S BOX?

Academic ☆☆☆ **Business** ☆ **Policy** ☆☆
Organised by University of Luxembourg (LU)
Moderator Mark Cole, University of Luxembourg (LU)
Speakers Vanessa Franssen, University of Liège and KU Leuven (BE); Stanisław Tosza, University of Luxembourg (LU); Erik Valgaeren, Stibbe (BE); Martyna Kusak, University of Poznań (PL); Marc van der Ham, National Office of the Dutch Prosecution Service (NL)

In January 2023 the EU legislators finally reached a compromise on the text of the E-Evidence Regulation (and its accompanying Directive). By the time this panel takes places the final adoption of these two instruments is expected. This ends a five-year legislative process and results in the creation of the European Production and Preservation Orders for cross-border gathering of electronic evidence for criminal proceedings, which are bound to become a major instrument of evidence gathering in the EU. The order is not without controversy and this panel will discuss some of the most pertinent issues: the real efficiency of the new system of e-evidence gathering, the role of the service providers as guardians of users' fundamental rights, e-evidence gathering by countries with rule of law-concerns, and the role of the order for the defence.

- To what extent does the E-Evidence Regulation effectively address the needs and problems encountered by police and judicial authorities with respect to cross-border gathering of digital evidence, and what will the interplay between the new EU legal regime and national (pre-existing) procedures be?
- What will the formal and de facto role of private actors (Internet service providers) in assessing the European production orders be?
- What challenges does gathering of electronic evidence face in the EU Member States where the independence of the judiciary is questioned?
- What opportunities and challenges does the new E-Evidence Regulation offer for the defence?
- What opportunities and challenges does the new E-Evidence Regulation offer for the investigating and prosecuting services?

13:00 - LUNCH

14:15 – WILL THE DIGITAL SERVICES ACT PROMOTE SAFER AND HEALTHIER ALGORITHMIC RANKINGS?

Academic ☆☆☆ **Business** ☆ **Policy** ☆☆
Organised by The Mozilla Foundation (US)
Moderator Maximillian Gahnz, The Mozilla Foundation (US)
Speakers Jesse McCrosky, Mozilla Foundation and Thoughtworks (IT); Xabier Lareo, European Data Protection Supervisor (EU); Francesco Ricci, Faculty of Engineering, Free University of Bozen-Bolzano (IT); Anna-Katharina Meßmer, Stiftung Neue Verantwortung (DE)

The Digital Services Act's Article 27 will require online platforms to inform their users about the main parameters used in their recommender systems and of the options to tweak those parameters. On the other hand, Article 38 will require the largest online platforms to provide an alternate recommender system not based on profiling as defined in the GDPR. What impact will this have on polarisation, hate speech, data protection risks, or other behavioural consequences that stem from personalised recommendations optimised for engagement? How will this affect transparency and user control?

The DSA already arrives at a time of increased discussion of chronological news feeds and research into alternative recommendation models, for instance through the opportunities of open-source and local/community governed models or through techniques like "bridging". It also comes at a moment of heightened scrutiny of social media platform recommender systems and efforts make them more transparent and accountable.

- Will the DSA truly create space for alternatives, and how will we assess these alternatives?
- How can a satisfactory user profile be constructed and maintained while respecting the regulatory requirements and balancing potentially conflicting interests?

This discussion will weigh the technical possibilities for widespread uptake and debate the potential individual and societal benefits as well as the risks and trade-offs.

15:30 - COFFEE BREAK

16:00 – THE REGULATION OF ONLINE ADVERTISING, BETWEEN THE GDPR AND THE DSA

Academic ☆☆☆ **Business** ☆ **Policy** ☆☆
Organised by IVIR - DSA Observatory, University of Amsterdam (NL)
Moderator Mathias Vermeulen, AWO Agency (BE)
Speakers Maryant Fernandez, BEUC (BE); Christian D'Cunha, European Commission (BE); Ruth Boardman, Bird and Bird (UK) Ilaria Buri, University of Amsterdam (NL)

The DSA debate started very ambitious on the idea of introducing significant limitations to the data-intensive business models underlying much of the platform economy today. As the political process unfolded, the data protection-related aspects of the DSA (tracking-based advertising in particular) become some of the most lobbied provisions in the draft regulation. Amongst others, the EDPS and EDPB indicated that the DSA proposal needed a more radical approach towards the data practices of the online platforms. The final text, however, landed on more limited set of restrictions. Against this background, a number of interesting and complex questions arise, which are worth discussing.

- What can we expect from the synergy of the GDPR and the DSA when it comes to privacy and data protection across (very large) online platforms in particular?
- How will the societal systemic risk rules play out with regard to some of the most problematic aspects of the business models underlying online platforms?
- Will access to data for researchers and auditing concretely shade any light on the functioning and systemic societal risks posed by platforms systems?
- What are the lessons we can draw from the DSA process on the future of data protection and its enforcement?

17:15 – THE GOVERNANCE OF AI: CONVERGENCE OR DIVERGENCE?

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by Center for AI and Digital Policy (US)
Moderator Merve Hickok, Center for AI and Digital Policy (US)
Speakers Emilio De Capitani, former Civil Liberties Committee (LIBE) of the European Parliament (EU); Daniel Leufer, Access Now (BE); Eleni Kosta, TILT, Tilburg University (NL); Tjade Stroband, Microsoft (BE)

As more AI national strategies emerge and more global frameworks are adopted, there appears to be an emerging consensus for the governance of AI. Key concepts, such as fairness, transparency, and accountability are now the pillars of modern AI policy. But additional issues, such as gender equity and sustainability are emerging, while some countries are still struggling with regulation for basic concepts. What is the path ahead? In this panel, we will explore these key topics:

- Where are we seeing commonality in AI policy frameworks? What are the core tenants for the governance of AI?
- What do we do with the countries that have yet to establish these base line principles?
- Do we anticipate a Brussels Effect following adoption of the EU AI Act?
- In the risk-based governance models, how do we ensure protection of fundamental rights?

FRIDAY 26 MAY 2023

18:30 – CLOSING REMARKS BY WOJCIECH WIEWIOROWSKI (EPDS) AND CHRISTOPHER KUNER (VUB)

in Grande Halle

19:00 – COCKTAIL SPONSORED BY PRIVACY SALON

in Le Village

CPDP2023 PANELS AT LA CAVE

08:45 – ACCOUNTABILITY TOOLS: FROM TRANSFERS TO CROSS-BORDER INTEROPERABILITY

Academic ☆ **Business** ☆☆☆ **Policy** ☆☆
Organised by CIPL (EU)
Moderator Marie-Charlotte Roques-Bonnet, ID Side Consulting (FR)
Speakers Nicola Coogan, Ireland's Data Protection Commission (IE); Bojana Bellamy, CIPL (UK); Fabrice Naftalski, EY (FR)

Experienced representatives of different EU, EMEA and international organisations reflect on their (mainly EU-centred) experience about data transfers in theory and data transfers in practice. Contrary to other panels on the topic, the objective of this panel will not be to discuss Schrems nb 1, 2, 3… or n, but to envisage in practice whether, in 2023, accountable exporters and importers are:

1. addressing a set of "equivalent" legal obligations worldwide;
2. equipped, in different regions of the world, with accessible and efficient tools -or in need for a more flexible approach and real-life compatible set of processes;
3. in capacity to leverage their accountability programs, processes, procedures and documents for doing so. To explore existing and upcoming solutions, this panel will navigate among the practical viewpoints and real-life experiences from senior regulators, practitioners, business consultants and experts.

Questions addressed will notably be:

- What are the practical solutions that accountable stakeholders could explore to keep transferring personal data and mitigating data transfers' risks?
- What's the germinating notion of "Accountable Data Transfer" (reference to the best of Accountability tools and specifically CBPRs, BCRs and Privacy Management Programs)?
- What's the difference between what's expected "by the books" and what can possibly be accomplished "in reality" by accountable companies benefitting from both extended resources and a genuine commitment to Privacy?
- What small and medium-sized accountable bodies with limited resources can achieve in practice, and how they should rethink

10:00 - COFFEE BREAK

10:30 – EU-US DATA PRIVACY FRAMEWORK: HOW DOES THE US EO SUSTAIN A NEW DURABLE AGREEMENT?

Academic ☆☆☆ **Business** ☆ **Policy** ☆☆
Organised by CEU San Pablo University (ES) - South EU Google Data Governance Chair (EU)
Moderator José Luis Piñar - CEU San Pablo University (ES)
Speakers Vincenzo Zeno-Zencovich, RomaTre University (IT); Maria da Graça Canto, Nova University Lisbon (PT); Georgios Yannopoulos, National and Kapodistrian University of Athens (GR); Isabelle Roccia, IAPP Europe (BE)

This panel will discuss on the reflection that arose following the adoption of the Executive Order, with the status of law, approved by President Biden with the aim to take a step forward in facilitating international data transfers between the European Union and the United States. A scenario is opening up before us in which a new framework is likely to be drawn up that will regulate international data flows on both sides of the Atlantic for the coming years.

The essential question to be asked at this point with respect to the current EU-US Data Privacy Framework is what element can ensure that this new context brings with it a stable agreement that can be maintained over time. Other questions the panel will discuss include:

- How to ensure that the new framework will fully address fundamental rights issues ?
- What does the future look like following the negative opinion of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs on the European Commission's proposal for an adequacy decision on the EU-US Data Privacy Framework ?
- Will Privacy Shield 2.0 survive ?
- What could be the essential element in the consolidation of an acceptable framework for personal data flows between the EU and the US ?
- Are the safeguards included in the EO, regarding the substantive limitation on US national security authorities access to personal data and the establishment of a redress mechanism, the optimal elements to ensure the success of the new framework ?

11:45 – "FLEXIBILITY" IN THE "ESSENTIAL EQUIVALENCE" TEST FOR DATA TRANSFERS: TAKING INTO ACCOUNT DIFFERENT LEGAL TRADITIONS AND CONSTITUTIONAL CONSTRAINTS IN THIRD COUNTRIES

Academic ☆☆☆ **Business** ☆ **Policy** ☆☆
Organised by The School of Cybersecurity & Privacy, Georgia Institute of Technology (US)
Moderator Théodore Christakis, Université Grenoble Alpes (FR)
Speakers Anna Buchta, European Data Protection Supervisor (EU); Nora Ni Loideain, Institute of Advanced Legal Studies, University of London (UK); Peter Swire, Georgia Institute of Technology (US)

In Schrems II, Advocate General Oe, wrote that "The 'essential equivalence' test should be applied in such a way as to preserve a certain flexibility in order to take the various legal and cultural traditions into account". During the EU-US negotiations about Privacy Shield several areas of tension appeared between the constitutional constraints of US law and EU fundamental rights requirements, including for standing to sue in U.S. federal court, and the role of the President in national security. The panel examines what happens when a third country's constitution operates differently from the expectation of EU law, in light of the high standards of EU law. Drawing on the jurisprudence of the Strasbourg and Luxembourg courts, the panel seeks to generate a profound discussion on the concept of "essential equivalence" as applied to possible constitutional conflicts of law.

- What if any are U.S. constitutional doctrines that may conflict with EU fundamental rights law?
- How might EU law generally address conflicts of constitutional law?
- How might "essential equivalence" be interpreted in the face of constitutional differences with third countries?
- What options would exist for next steps if the requirements of EU law would require constitutional change in a third country?

13:00 - LUNCH

14:15 – ENDING THE PRIVACY OF THOSE WHO ARE SUPPOSED TO BE PROTECTED OR EFFECTIVELY SAFEGUARDING CHILDREN AGAINST ONLINE SEXUAL ABUSE?

Academic ☆☆ **Business** ☆ **Policy** ☆☆☆
Organised by European Centre on Privacy and Cybersecurity (ECPC) (NL)
Moderator Teresa Quintel, European Centre on Privacy and Cybersecurity (ECPC) (NL)
Speakers Cathrin Bauer-Bulst, DG for Migration and Home Affairs (EU), Thomas van de Valk, Meta (US); Alexander Hanff, Privacy Consultant (SE); Arda Gerkens, Expertisebureau Online Kindermisbruik (EOKM) and Dutch Senate, first chamber (NL); Cosimo Monda, ECPC (NL)

On 11 May 2022, the EU Commission proposed a regulation on preventing and combating child sexual abuse. The proposal lays down rules allowing national authorities to mandate service providers to detect, block, delete and report known and new child sexual abuse material including the solicitation of children. The Proposal applies to virtually all online platforms and interpersonal communication services in the EU and would thus, have an impact on practically all online activity. The panel will discuss concerns around the proposal and what impact the proposed rules will have on the privacy of users in practice. In particular, the panelists will look at the protection of children and their right to human dignity and privacy, but also the positive obligation to ensure a safe environment for them in the digital world and whether the proposal could effectively achieve its objective.

- What impact has the CSA proposal on children's right to human dignity and privacy?
- Is the CSA proposal ending the privacy of those who are supposed to be protected or effectively safeguarding children against online sexual abuse?
- What is the impact of the CSA proposal on digital activity, including private communication of users?
- To what extent are the rights and obligations provided for in the e-Privacy Directive (confidentiality of communications) restricted by analogy of Article 15(1) of the e-Privacy Directive?

15:30 - COFFEE BREAK

16:00 – FROM SCIENCE FICTION TO REALITY: THE ETHICS OF BODY-TECHNOLOGY INTERACTIONS

Academic ☆ **Business** ☆☆ **Policy** ☆☆☆
Organised by IMPAKT (NL), Privacy Salon (B), Werktank (B) and transmediale (D), as part of CODE.
Moderator Eduard Fosch-Villaronga, Leiden University (NL)
Speakers Sander Veenhof, Independent Artist (NL); Ahnjili Zuparris, PhD researcher in Advanced Data Analytics, freelance data scientist and communicator (US); John Mulgrew, Lenovo (US); Hans Graux, Timelex / Flemish Supervisory Committee (BE)

Advancements in digital technologies have revolutionized the way we interact with our environment, particularly in the field of Virtual Reality (VR), Augmented Reality (AR), Brain-Computer Interfaces (BCI), and Healthcare. However, as these technologies develop, they raise questions about our bodies being commodified, and the implications this may have on our physical integrity, privacy, safety, and dignity.

This panel discussion will bring together artists and law and technology experts to explore the challenges brought to us by recent advancements in VR, AR, BCI, and the health industry and the impact of these advancements on our bodies. The panelists will also discuss the importance of ensuring that our voices, gestures, and movements are not commodified or exploited for profit-driven competitions for patents and what role art has in these advancements.

The panel will explore the following questions:

- How can we ensure that using VR, AR, BCI, and technology in healthcare and other industries does not compromise our user rights, privacy, autonomy, and dignity?

- How do patent laws and intellectual property rights impact the development of these technologies, and what are the ethical implications of these laws?
- With ongoing innovations in healthcare forms of technology get closer connected, sometimes even inserted in our bodies. How does the integration of more and more sensors into our own bodies influence the discussion around rights, privacy, autonomy and dignity?
- How can art be effectively used as a platform for communicating complex ethical and social issues related to emerging technologies to a broader audience, encouraging dialogue, and engaging diverse perspectives?
- What are some strategies for leveraging art to support policy formation, promote public engagement and reflection, and participatory approaches to developing emerging technologies?
- How can artists, policymakers, technologists, and ethicists collaborate to create works and approaches that challenge and explore these technologies' ethical and social implications?

17:15 – ACCOMMODATING CHILDREN'S NEEDS ONLINE: AN IMPOSSIBLE TASK?

Academic ☆☆☆ **Business** ☆ **Policy** ☆☆
Organised by Computer Law & Security Review (CLSR) (UK)
Moderator Sophie Stalla-Bourdillon, University of Southampton (UK)
Speakers Martin Bieri, CNIL (FR); Eva Lievens, Ghent University (NL); Eric Goldman, Santa Clara Law School (US) ; Tony Allen, ACCS Scheme (UK)

The data deluge is affecting both adults and children. However, with youngsters challenges become much more acute: a huge quantity of data spanning their entire lifetime is being accumulated, while they are not well equipped to understand the implications of the data collection and processing operations happening on the backend of online services. Besides, in the age of personalisation and automation, it seems relatively easy to fall into the trap of harmful content and suffer irreversible damage as a result. This explains why minors and children have been acknowledged in a variety of recent pieces of legislation and regulatory guidance. But are lawmakers on the right track? Have they carefully considered the range of options available? Can privacy enhancing technology help with identifying the least intrusive means?

- What is the EU strategy on the matter and how has it been pursued in the latest regulatory package?
- What are the lessons learned from the ICO Appropriate Age Design Code of Practice?
- What do the California lawmakers hope to achieve with the new Appropriate Age Design Act?
- What are the benefits and drawbacks of age verification solutions?

18:30 – CLOSING REMARKS BY WOJCIECH WIEWIOROWSKI (EPDS) AND CHRISTOPHER KUNER (VUB) in Grande Halle

19:00 – COCKTAIL SPONSORED BY PRIVACY SALON

in Le Village

CPDP2023 PANELS AT AREA 42 PETITE

08:45 – ACHIEVING SOCIAL JUSTICE FOR DATA WORKERS: IS THERE A ROLE FOR HARMONISED STANDARDS?

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by European Trade Union Institute (EU)
Moderator Jill Toh, University of Amsterdam (NL)
Speakers Antonio Casilli, Télécom Paris, Polytechnic Institute of Paris (FR); Laurens Hernalsteen, CEN CENELEC (EU); Iverna McGowan, Centre for Democracy and Technology (BE); Aida Ponce Del Castillo, European Trade Union Institute (BE)

The development of a "human-centered" AI tends to overlook a component of AI development: data production. Machine learning data sets are used to develop and train algorithms. The resulting algorithms are then used for content moderation, facial recognition, or to train self-driving cars, etc. The amount of data needed for this, has to be sorted, cleaned, annotated, labelled. These tasks are far from automated: they are outsourced to manual labor in countries where wages and working conditions are low. From a data justice perspective, is this reality considered when thinking about regulating AI? Issues related to the exploitation of labour, social justice and power remain unaddressed. In the EU, the 8 legal requirements in the draft AI Act will be operationalized through harmonized standards. We will reflect about the ability of standardization committees to address the issue of data justice.

- In the debate about how best to regulate AI, is there space for a "social and data justice" perspective?
- Should the draft AI Act address this issue? In what way?
- Is there a possibility in the standardization committees to address the issue of data justice for data workers?
- Should standardization bodies be "revisited" in their membership, mandate and production process in order to address this issue?

10:00 - COFFEE BREAK

10:30 – ACADEMIC SESSION 1

Academic ☆☆☆☆☆☆
Organised by CPDP
Moderator Eleni Kosta, Tilburg University (NL)

- Amir Cahane, Hebrew University of Jerusalem (IL) - Creeping on: Israel's turn to counterterrorism measures during the pandemic
- Shrutika Gandhi, Institute of Advanced Legal Studies, University of London (UK) - FRONTEX as a hub for surveillance and data sharing: challenges for data protection and privacy rights
- Audrey Dequesness, University of Lille (FR) - Data as electronic evidence in criminal investigations: The legal framework for collection from service providers in a fragmented judicial Europe.

11:45 – ACADEMIC SESSION 2

Academic ☆☆☆☆☆☆
Organised by CPDP
Moderator Colin Bennett, University of Victoria (CA)

- Julia Krämer, Erasmus University Rotterdam (NL) - The death of privacy policies: how app stores shape GDPR compliance of apps
- Klaudia Majcher, Vienna University of Economics and Business (AT) and Vrije Universiteit Brussel (BE) - Data protection as a justification of an abusive conduct: the EU competition law perspective
- Jan Czarnocki, KU Leuven (BE) - Addressing legitimacy and data power through qualified transparency in the GDPR
- Karlo Lukic and Bernd Skiera, Goethe University Frankfurt (DE), and Klaus Miller, HEC Paris (FR) - The impact of the General Data Protection Regulation (GDPR) on online tracking

13:00 - LUNCH

14:15 – ACADEMIC SESSION 3

Academic ☆☆☆☆☆☆
Organised by CPDP
Moderator Nina Baranowska, FINDHR Project, Radboud University (NL)

- Emmanouil Bougiakiotis, European University Institute (IT) - Control without consent: bridging the gap between individualistic and collective data protection governance
- Merel Noorman, Tilburg University (NL) and Tsjalling Swierstra, Maastricht University (NL) - Democratizing AI from a sociotechnical perspective
- Ero Balsa and Helen Nissenbaum, Cornell Tech (US) - Technocracy, pseudoscience & performative compliance: the risk of privacy risk assessments. Lessons from NIST's Privacy Risk Assessment Methodology
- CNIL/INRIA privacy award winner

15:30 - COFFEE BREAK

16:00 – NOVEL CONCEPTS IN DIGITAL STATES AND THEIR STRUCTURES

Academic ☆☆☆☆ **Business** ☆ **Policy** ☆
Organised by CDSL
Moderator Alessandro Mantelero, University of Turin (IT)
Speakers Indra Spiecker genannt Döhmann, University of Frankfurt (DE); Dara Hallinan, FIZ Karlsruhe (DE); Vagelis Papakonstantinou, Vrije Universiteit Brussel (BE)

The role of states is fundamentally challenged in the digital realm. Westphalian nation states, built on 19th century notions of sovereignty and statehood, witness their roles, premises and basic assumptions questioned as the virtual, digital world complements the real, analogue environment.

Constitutions are increasingly in need of digitisation (digital constitutionalism), data sovereignty seems a lost cause, citizens are allowed to become e-residents or digital nomads, digitally carrying out their lives and creating income in other, competing jurisdictions.

Challenges also come from outside: The digital environment allows large international corporations, that until recently had to establish local presence within any specific jurisdiction they wished to become active, to carry out business and realise income remotely, paying little attention to geographical borders and local laws.

States will therefore need novel concepts and new structures to assist them in their struggle to reaffirm their fitness for any purpose and safeguard their continued existence.

Four issues to be addressed by the panel:

- Digital states and digital statehood;
- Digital constitutionalism and new types of individual rights;
- Is data sovereignty (if considered a worthy cause) attainable?
- What is the role of states in the digital environment? States as platforms

17:15 – WORKING & MEETING SPACE

18:30 – CLOSING REMARKS BY WOJCIECH WIEWIOROWSKI (EPDS) AND CHRISTOPHER KUNER (VUB)

in Grande Halle

19:00 – COCKTAIL SPONSORED BY PRIVACY SALON

in Le Village

FRIDAY 26 MAY 2023

CPDP2023 WORKSHOPS AT M-VILLAGE GRANDE

08:45 – Workshop HOW TO BRING CONTROL BACK TO THE HUMANS BEINGS - ENLIGHTENING THE AI BLACK BOX

Organised by nexus Institut Berlin (DE)
Workshop facilitator Volkan Sayman, nexus Institut Berlin (DE); Cecilisa Colloseus

The problem of biased AI algorithms and their hazardous effects have come to the broad discourse. We still lack applicable tools and methods to empower operators and ensure the implementation of values-by-design. Often the discourse remains on an abstract level, but we will discuss hands-on solutions.

We invite a number of projects to shortly present their tools and approaches supported by concrete cases, followed by a world café: In small groups we will have two rounds of interactive discussions to address the applicability of approaches. We address explainability, human in control, participative development, algorithmic accountability and auditing.

Finally, each project presents its main learnings from the discussion.

- How to make AI transparent and understandable? If possible, does it strengthen control?
- How to minimise discrimination and bias?
- How to give users control over AI system's?
- How to hold organisations accountable?

10:00 - COFFEE BREAK

10:30 – Book Launch "VULNERABILITY AND DATA PROTECTION LAW" BOOK LAUNCH

Organised by "VULNERA" Observatory at the Brussels Privacy Hub (BE)
Workshop facilitator Paul De Hert, VUB (BE)
Speakers Wojciech Wieworoski, EDPS (EU); Julie Cohen, Georgetown University (US); Natali Helberger, UvA (NL)
Author Gianclaudio Malgieri, Leiden University (NL) and Vrije Universiteit Brussel (BE)

The aim of this session is to discuss the topic of the Book "Vulnerable People and Data Protection law" by Gianclaudio Malgieri, published by Oxford University Press on April 2023. The book addresses the issue of vulnerable data subjects in the GDPR and in related legislation. The book is a mere opportunity to discuss more in depth: the notion of the data subject, how gender studies could inform the data protection discussion on this and how to conduct a vulnerability-aware interpretation of the GDPR's principles, rights and duties.

- Who is the vulnerable data subject in the GDPR?
- How the notion of "power" is relevant to address the vulnerable data subject?
- How can gender studies help define vulnerability in the GDPR?
- Are the GDPR and the EU digital strategy compatible with a concept of layered and intersectional vulnerability?

11:45 – Workshop DARK PATTERNS FIGHTERS - UNITE!

Organised by SnT, University of Luxembourg
Workshop facilitators Kerstin Bongard-Blanchy, University of Luxembourg (LU); Arianna Rossi, SnT University of Luxembourg (LU); Anastasia Sergeeva, University of Luxembourg (LU)
Speakers Sarah Eskens, Vrije Universiteit Amsterdam (NL); Nataliia Bielova, INRIA (FR)

Many panels at the CPDP have been dedicated to deceptive design patterns, bringing together academia, SMEs, corporations, watchdogs, NGOs that work acrossdata protection, consumer and competition law, as well as human-centred design, digital ethics and privacy engineering. As the knowledge on online manipulation and the number of enforcing actions grow, we intend to exchange best practices, systematise knowledge and establish common goals. This interactive workshop will recap the main takeaways of the CPDP23 panels about deceptive design and plan the next actions we need to undertake as a community to fight dark patterns.

- How might we capitalise on the existing knowledge about dark patterns?
- How might we best strategise and coordinate the actions of our community?
- Which solutions against dark patterns exist and which ones should we create?
- What is one common goal that we can achieve in 2023?

13:00 - LUNCH

14:15 – Workshop THE RIGHT OF ACCESS TO POLICE DATABASES

Organised by Vrije Universiteit Brussel
Workshop facilitator Franck Dumortier, VUB (BE)
Speakers Catherine Forget, Université Saint-Louis (BE); Joanna Parkin, EDPS (EU); Daniel Drewer, Europol (DE); Stergios Konstantinou, Homo Digitalis (GR)

Directive 2016/680 grants data subjects the right to directly access personal data processed by police forces. Nevertheless, in order to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences, restrictions may be taken to proportionally limit such a right and provide the possibility of exercising such a right through the supervisory authority. In the pending case C-333/22, the ECJ is currently examining the compatibility of the Belgian system of systematic indirect access through the supervisory authority with the abovementioned Directive. The aim of the panel is to compare different national and organizational (Europol) legal regimes to identify the ideal path to guarantee the preservation of fundamental rights of citizens while ensuring that police forces can efficiently do their work.

- How should the limitations to the rights of information and access to police databases be applied so as to ensure proportionality ?
- What is the role of a supervisory authority in ensuring that limitations to such rights are proportional ? What value do their decisions have ?
- Which are the judicial remedies against decisions of the supervisory authorities ?
- Is a national system of systematic indirect access through the supervisory authority which will simply inform the data subject that 'the necessary verifications have been carried out' compatible with Directive 2016/680 ?

15:30 - COFFEE BREAK

16:00 – Workshop A GDPR CERTIFICATION JOURNEY IN PRACTICE: HOW TO PREPARE FOR A EUROPRIVACY AUDIT AND THE ACTUAL CERTIFICATE

Organised by Timelex (BE)
Workshop facilitator Geert Somers, Timelex (BE)
Speakers Pieter Gryffroy, Timelex (BE), Giovanni Francescutti, DNV (IT); Sebastien Ziegler, Mandat International

In this workshop we will explain GDPR certification and discuss 2 practical cases under the first EU wide certification scheme Europrivacy. Together with the audience, we will examine how to start and scope the journey, including a good definition of the Target of Evaluation. We will also look at the documentation that needs to be in place to meet the Europrivacy criteria. And last but not least, we will give our perspectives on the added-value of GDPR certification over the next years. The audience will have the opportunity to provide feedback and asks questions.

17:15 – WORKING & MEETING SPACE

18:30 – CLOSING REMARKS BY WOJCIECH WIEWIOROWSKI (EPDS) AND CHRISTOPHER KUNER (VUB)

in Grande Halle

19:00 – COCKTAIL SPONSORED BY PRIVACY SALON

in Le Village

CPDP2023 WORKSHOPS AT M-VILLAGE MIDI

FULL DAY SESSION – REGISTRATION ONLY

08:45 – Seminar PHILOSOPHERS' SEMINAR ON COMPLIANCE AND AUTOMATION IN DATA PROTECTION LAW [ENDS AT 17:00]

Organised by CPDP, ALTEP-DP and COHUBICOL (BE)
Limited participation participants must be registered in advance for this session by sending an email to Gianmarco.Gori@vub.be.
Hosted by Mireille Hildebrandt and Gianmarco Gori VUB-LSTS (BE) and Radboud University (NL)
Confirmed authors Roger Brownsword; Federico Cabitza; Tatiana Duarte;Massimo Durante; Orla Lynskey; Thomas Troels Hildebrandt; Gabriela Zanfir
Find out more at https://www.cohubicol.com/about/philosophers-seminar-2023?

Participants are expected to have read the texts under discussion which will be disseminated in advance. Since the very first CPDP Conference (2009), a distinctive though unobtrusive – slow science - seminar has been organized four times. The idea is to think and rethink the constitutive impact of our information and communication technological infrastructures (ICIs), notably assessing the transitions from speech, writing and printing towards a networked computational order that pervasively measures anybody's and anything's machine-readable behaviours, while remaining agnostic as to meaningful action. This time the seminar will engage with attempts to automate legal protection, notably in the context of the GDPR. All previous philosophers' seminars have resulted in edited volumes (one also in a special issue): Law, Human Agency and Autonomic Computing (Routledge 2011) and Privacy, Due Process and the Computational Turn (Routledge 2013), Information, freedom and property (Routledge 2015), Special Issue Critical Analysis of Law (2017) and Life and the Law in the Era of Data-Driven Agency (Edward Elgar 2019).

FRIDAY 26 MAY 2023

CPDP2023 Sponsors

PLATINUM SPONSORS

APPLE

Apple revolutionized personal technology with the introduction of the Macintosh in 1984. Today, Apple leads the world in innovation with iPhone, iPad, Mac, Apple Watch and Apple TV. Apple's five software platforms — iOS, iPadOS, macOS, watchOS and tvOS — provide seamless experiences across all Apple devices and empower people with breakthrough services including the App Store, Apple Music, Apple Pay and iCloud. Apple's more than 100,000 employees are dedicated to making the best products on earth, and to leaving the world better than we found it.

EUROPEAN DATA PROTECTION SUPERVISOR (EDPS)

The European Data Protection Supervisor is an independent supervisory authority, with responsibility for monitoring the processing of personal data by the EU institutions and bodies, advising on policies and legislation that affect privacy and cooperating with similar authorities at national level. The EDPS remit includes:

- developing and communicating an overall vision, thinking in global terms and proposing concrete recommendations;
- providing policy guidance to meet new challenges in the area of data protection;
- operating at the highest levels and developing effective relationships with diverse stakeholders in other EU institutions, Member States, non EU countries and other national or international organisations.

GOOGLE

Google's mission is to organize the world's information and make it universally accessible and useful. Through products and platforms like Search, Maps, Gmail, Android, Google Play, Chrome and YouTube, Google plays a meaningful role in the daily lives of billions of people and has become one of the most widely-known companies in the world. Google is a subsidiary of Alphabet Inc.

LES HALLES DE SCHAERBEEK

Ever since their beginnings, Les Halles have captured and crystallised movements stemming right from the edges of art and society, in an unprecedented alliance of both learned and popular culture. Open to contemporary hopes and upheavals spanning from the neighborhood right out to the world at large, Les Halles keep on looking for what Europe, still on a quest for its own destiny, has to offer: exploration of new passions, reason seeking out adventure, the utmost freedom of style. Les Halles resonate with a desire for participation and involvement, be it individually or collectively, thus characterising the digital age.

META

Meta builds technologies that help people connect, find communities, and grow businesses. When Facebook launched in 2004, it changed the way people connect. Apps like Messenger, Instagram and WhatsApp further empowered billions around the world. Now, Meta is moving beyond 2D screens toward immersive experiences like augmented and virtual reality to help build the next evolution in social technology.

MICROSOFT

Microsoft enables digital transformation for the era of an intelligent cloud and an intelligent edge. Its mission is to empower every person and every organization on the planet to achieve more.

PREMIER SPONSORS

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA)

The European Union Agency for Fundamental Rights (FRA), established by the EU as one of its specialised agencies in 2007, provides independent, evidence-based advice on fundamental rights to the institutions of the EU and the Member States on a range of issues. The staff of the FRA, which is based in Vienna, includes legal experts, political and social scientists, statisticians, and communication and networking experts.

KINESSO

Kinesso builds advanced and adaptable marketing intelligence technology to connect people and grow brands. We enable a world where every connection between brands and customers is meaningful.

MOZILLA

Mozilla's mission is to promote openness, innovation and opportunity on the web. We produce the Firefox web browser and other products and services, together adopted by hundreds of millions individual internet users around the world. Mozilla is also a non-profit foundation that educates and empowers internet users to be the web's makers, not just its consumers. To accomplish this, Mozilla functions as a community of technologists, thinkers, and builders who work together to keep the Internet alive and accessible.

TIKTOK

TikTok is the entertainment destination where the everyday meets the extraordinary. Discover, watch, create, and share what you love with a global community. We take the privacy and security of the people who use TikTok seriously. We're working toward charting a new course for the industry when it comes to data security, and we're reflecting this in our evolving approach to European data sovereignty, including storing UK and EEA user data locally in Europe.

UBER

Good things happen when people can move, whether across town or towards their dreams. Opportunities appear, open up, become reality. What started as a way to tap a button to get a ride has led to billions of moments of human connection as people around the world go all kinds of places in all kinds of ways with the help of our technology.

WORKDAY

Workday is a leading provider of enterprise cloud applications for finance and human resources, helping customers adapt and thrive in a changing world. Workday applications for financial management, human resources, planning, spend management, and analytics are built with artificial intelligence and machine learning at the core to help organizations around the world embrace the future of work. Workday is used by more than 10,000 organizations around the world and across industries—from medium-sized businesses to more than 50% of the Fortune 500.

BIRD & BIRD

Bird & Bird LLP is an international law firm which supports organisations being changed by the digital world or those leading that change. We combine exceptional legal expertise with deep industry knowledge and refreshingly creative thinking, to help clients achieve their commercial goals. We have over 1300 lawyers in 29 offices across Europe, North America, the Middle East and Asia Pacific, as well as close ties with firms in other parts of the world.

BRAVE

Brave is on a mission to protect your privacy online. We make a suite of internet privacy tools—including our browser and search engine —that shield you from the ads, trackers, and other creepy stuff trying to follow you across the web

BSA | THE SOFTWARE ALLIANCE

BSA | The Software Alliance is the leading advocate for the global software industry. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC and operations in more than 30 countries around the world, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)

EPIC is an independent non-profit research center in Washington, DC. EPIC protects privacy, freedom of expression, and democratic values; and promotes the Public Voice in decisions concerning the future of the Internet. EPIC's program activities include public education, litigation, and advocacy. EPIC files amicus briefs, pursues open government cases, defends consumer privacy, and testifies about emerging privacy and civil liberties issues.

EYEO

At eyeo, we transform the internet into a trusted, safe and accessible place where people regain control over their experience, content creators and publishers are rewarded for their content, and advertisers and consumers can connect on mutually agreed terms.
Our 250+ employees are distributed worldwide, working remotely, or housed in one of our offices in Cologne, Berlin, or Malmö. We develop and provide a suite of innovative products and services, with our flagship ad-filtering technology powering some of the largest ad blockers on the market, like Adblock Plus and AdBlock, and our Acceptable Ads Standard reaching over 250 million online users.

IEEE STANDARDS ASSOCIATION

The IEEE Standards Association (IEEE SA) is a leading consensus-building organization that nurtures, develops, and advances global technologies. Providing a neutral and open platform to empower innovators across borders and disciplines, IEEE SA facilitates standards development and standards-related solutions, such as technology incubation, alliance consortia formation, open-source, etc. With thought leaders in more than 160 countries, we enable the collaborative exploration of emerging technologies, the identification of existing challenges and opportunities, and the development of recommendations, solutions, and technology standards that solve market-relevant problems. Collectively, we are raising the standards that benefit industry and humanity; making technology better, safer, and more sustainable for the future.

HOGAN LOVELLS INTERNATIONAL LLP

Straight talking. Thinking around corners. Understanding and solving the problem before it becomes a problem. Performing as a team, no matter where we're sitting. Delivering clear and practical advice that gets your job done. Our 2,500 lawyers work together, solving your toughest legal issues in major industries and commercial centers. Expanding into new markets, considering capital from new sources, or dealing with increasingly complex regulation or disputes - we help you stay on top of your risks and opportunities. Around the world.

INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (IAPP)

The International Association of Privacy Professionals is the largest and most comprehensive global information privacy community and resource, helping practitioners develop and advance their careers and organizations manage and protect data. Founded in 2000, the IAPP is a not-for-profit association that helps define, support and improve the privacy profession globally.

MCDERMOTT WILL & EMERY

McDermott Will & Emery partners with leaders around the world to fuel missions, knock down barriers and shape markets. With 20+ locations globally, our team works seamlessly across practices, industries and geographies to deliver highly effective—and often unexpected—solutions that propel success. More than 1,400 lawyers strong, we bring our personal passion and legal prowess to bear in every matter for our clients and the people they serve.

NYM

Nym is a decentralised privacy system made up of a global mixnet, anonymous credentials and a blockchain. Founded in the aftermath of the Edward Snowden revelation, Nym's mission is to protect against network level surveillance and establish privacy as a default for online communications. Only then can people and organisations make meaningful and secure decisions about what, when and with whom they want to share data.

STIBBE

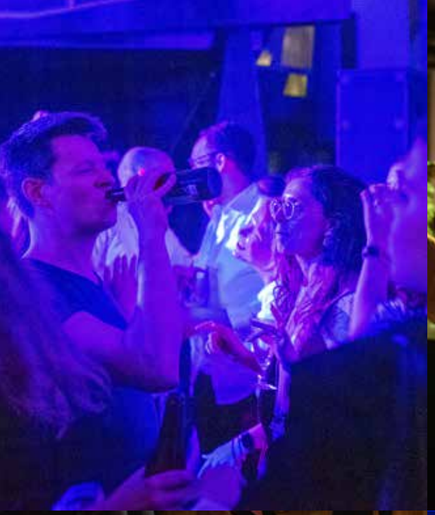
Stibbe's team of privacy and data protection specialists provides its clients with insight, foresight and experienced pragmatism. The team has over 20 years of experience in dealing with data protection authorities from different jurisdictions. The team is embedded in Stibbe's TMT practice (Technology Media and Telecoms), and, as a result, the members have a thorough understanding of information technology and data communication networks. The team is involved in data governance protection projects for national and international clients, covering an a broad range sectors, such as media/entertainment, finance, communications, industry and transport, consumer goods, government and healthcare. Typical projects include privacy health checks, corporate data exchange and monitoring programs and policies.

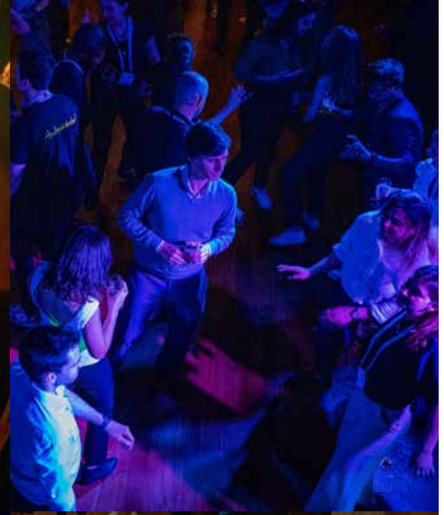
SQUIRE PATTON BOGGS

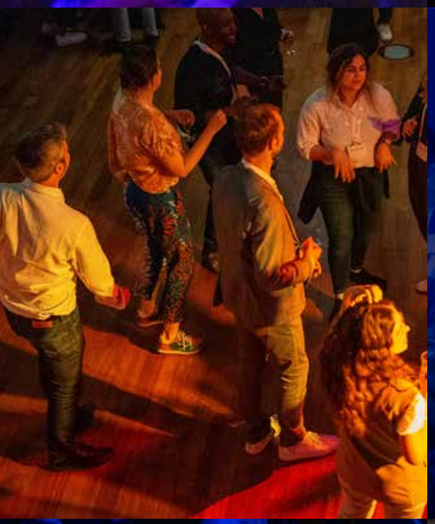
Squire Patton Boggs is one of the world's strongest integrated law firms, providing insight at the point where law, business and government meet. The firm delivers commercially focused business solutions by combining legal, lobbying and political capabilities and invaluable connections on the ground to a diverse mix of clients from long established leading corporations to emerging businesses, startup visionaries and sovereign nations. With more than 1,500 lawyers in 47 offices across 20 countries on five continents, Squire Patton Boggs provides unrivalled access to expertise.

WILSON SONSINI GOODRICH & ROSATI

Wilson Sonsini Goodrich & Rosati is a global law firm that helps clients maintain the highest standards for data protection while successfully pursuing their business interests. We have a fully integrated global practice with substantial experience in advising companies on all facets of global and EU privacy laws, including on topics such as big data, connected cards, cloud computing, and the Internet of Things. We have unique experience with complex multi-jurisdictional privacy investigations, enforcement actions, and litigation. We also counsel clients on the review of the EU data protection legal framework.



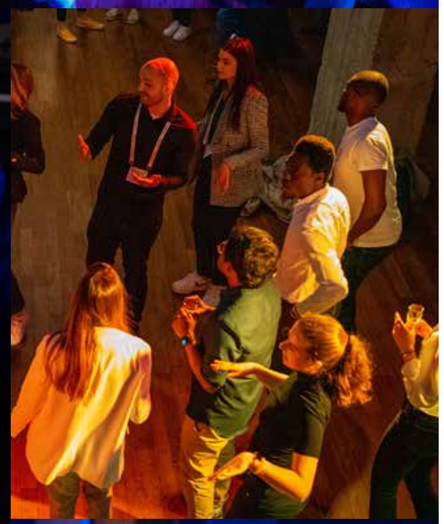


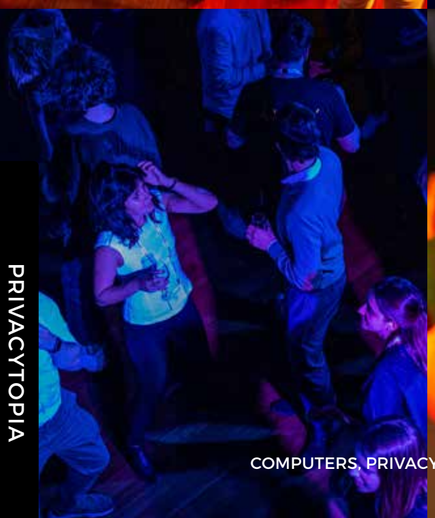


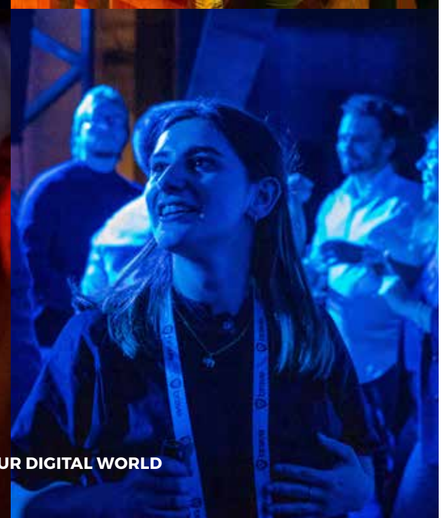
MOZILLA PARTY

We are delighted to announce the Official Party of CPDP2023, supported by Mozilla. We invite you to an evening of drinks, food and of course – to occupy the dancefloor to the tunes brought to you by Belgian pop dance duo Blondy Brownie.

Downstairs in Area42 on Thursday 25th May 2023 – 20:00 until late.







PRIVACYTOPIA

CPDP2023 SPONSORS & PARTNERS

EVENT PARTNERS

EVENT PARTNERS

WORKSHOP PRTNRS

MORAL SUPPORTERS

MEDIA PARTNERS

CPDP2023 SPONSORS & PARTNERS

PLATINUM

PREMIER

EVENT SPONSORS

INFO, PROGRAM & REGISTRATION: WWW.CPDPCONFERENCES.ORG

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

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

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