Organisation of CPDP2021

DIRECTORS
- Paul De Hert (Vrije Universiteit Brussel LSTS, Tilburg University TILT), Director and Founder
- Rosamunde Van Brakel (Vrije Universiteit Brussel LSTS), Managing director
- Dara Hallinan (FIZ Karlsruhe – Leibniz Institute for Information Infrastructure), Programme director

DAILY COORDINATORS
- Imge Ozcan (Vrije Universiteit Brussel LSTS)
- Thierry Vandenbussche (Privacy Salon)
- Diana Dimitrova (FIZ Karlsruhe – Leibniz Institute for Information Infrastructure)

CORE PROGRAMMING COMMITTEE
- Paul De Hert (Vrije Universiteit Brussel LSTS, Tilburg University TILT)
- Dara Hallinan (FIZ Karlsruhe – Leibniz Institute for Information Infrastructure)
- Rosamunde Van Brakel (Vrije Universiteit Brussel LSTS)
- Imge Ozcan (Vrije Universiteit Brussel LSTS)
- Diana Dimitrova (FIZ Karlsruhe – Leibniz Institute for Information Infrastructure)
- Magda Brewczyńska (Tilburg Institute for Law, Technology, and Society TILT)

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

PANEL COORDINATORS
- Alessandra Calvi (Vrije Universiteit Brussel LSTS)
- Katerina Demetrou (OD&R Business and Law Research Centre)
- Olga Giotopoulou (Vrije Universiteit Brussel LSTS)
- Lina Jasmonaité (Vrije Universiteit Brussel LSTS)
- Ana Fernandez (Vrije Universiteit Brussel LSTS)
- Sajedeh Salehi (Vrije Universiteit Brussel LSTS)
- Andrés Chomczyk Penedo (Vrije Universiteit Brussel LSTS)
- Bram Visser (Vrije Universiteit Brussel LSTS)
- Simone Casiraghi (Vrije Universiteit Brussel LSTS)
- Ashwnee Kumar (Vrije Universiteit Brussel LSTS)
- Georgios Bouchagiar (University of Luxembourg)
- Nikolaos Ioannidis (Vrije Universiteit Brussel LSTS)
- Guillermo Lazoza (Unversidad del Pais Vasco (UPV/EHU))

SCIENTIFIC COMMITTEE
- Rocco Bellanova, University of Amsterdam (NL)
- Franziska Boehm, Karlsruhe Institute of Technology, FIZ Karlsruhe – Leibniz Institute for Information Infrastructure (DE)
- Ian Brown, Research ICT Africa (SA)
- Paul De Hert, Vrije Universiteit Brussel LSTS (BE), Tilburg University TILT (NL)
- Willem Debreuckelaere, Ghent University (BE)
- Claudia Díaz, Katholieke Universiteit Leuven (BE)
- Michael Friedewald, Fraunhofer Institut Für System- Und Innovationsforschung ISI (DE)
- Serge Gutwirth, Vrije Universiteit Brussel LSTS (BE)
- Marit Hansen, Independent Centre For Privacy Protection ULD (DE)
- Mireille Hildebrandt, Radboud Universiteit Nijmegen (Netherlands) & Vrije Universiteit Brussel LSTS (BE)
- Dennis Hirsch, Ohio State University Moritz College of Law (US)
- Gus Hosein, Privacy International (UK)
- Kristina Irion, Institute for Information Law (IViR), University of Amsterdam (NL)
- Ets Kindt, Katholieke Universiteit Leuven Center for IT & IP Law (BE)
- Eleni Kosta, Tilburg Institute for Law, Technology and Society TILT (NL)
- Daniel Le Métayer, Institut National de Recherche en Informatique et en Automatique INRIA (FR)
- Ronald Leenes, Tilburg Institute for Law, Technology and Society TILT (NL)
- José-Luis Piñar, Universidad CEU-San Pablo (ES)
- Charles Raab, University of Edinburgh (UK)
- Marc Rotenberg, Center for AI and Digital Policy (US)
- Ivan Szekely, Central European University (HU)
- Frederik Zuiderveen Borgesius, Radboud University & IViR Institute for Information Law (NL)

LOGISTICS AND REGISTRATION

LOGISTICS AND ADMINISTRATIVE SUPPORT

Privacy Salon
www.privacysalon.org
Design © Nick Van Hee – www.nickvanhee.be
4 ENFORCING RIGHTS IN A CHANGING WORLD

CANCELLATION POLICY

For 3 days of participation we have an early bird fee until 30th of December 2011.

Each day is a self-contained conference and you can register to attend 1, 2 or all 3 days.

Any cancellation made after 4th of January 2012 will not receive a refund. Cancellation administration charge of € 50 will be made for all cancellations until 4th of January 2012.

REGISTRATION FEES

- General fee 250 euro, Student- & PhD-fee 130 euro
- Early Booking** 285 € (registration before 10 December 2010)
- General** 315 €
- Student 180 €

Books based on papers presented at previous CPDP conferences:


CPDP CONFERENCE BOOKS
<table>
<thead>
<tr>
<th>Time</th>
<th>Location</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.30</td>
<td>ONLINE 1</td>
<td>Welcome and Introduction by Paul De Hert</td>
</tr>
<tr>
<td>8.45</td>
<td>ONLINE 2</td>
<td>The use of AI in state surveillance: Challenges for privacy organised by TILT</td>
</tr>
<tr>
<td>8.45</td>
<td>ONLINE 3</td>
<td>Global Youth Privacy: Amplifying Youth Needs &amp; Voices organised by Privacy Salon</td>
</tr>
<tr>
<td>8.45</td>
<td>ONLINE 4</td>
<td>Algorithmic Criminal Justice organised by CPDP</td>
</tr>
<tr>
<td>10.00</td>
<td>ONLINE 1</td>
<td>Coffee break</td>
</tr>
<tr>
<td>10.30</td>
<td>ONLINE 2</td>
<td>Getting AI right – can data protection help safeguard other fundamental rights? organised by FRA</td>
</tr>
<tr>
<td>10.30</td>
<td>ONLINE 3</td>
<td>Ready for the next “Dieselgate” in data protection: the new reality of collective redress in the EU organised by Euroconsumers</td>
</tr>
<tr>
<td>10.30</td>
<td>ONLINE 4</td>
<td>Panel TBC organised by TBC</td>
</tr>
<tr>
<td>11.00</td>
<td>ONLINE 1</td>
<td>Getting AI right – can data protection help safeguard other fundamental rights? organised by FRA</td>
</tr>
<tr>
<td>11.00</td>
<td>ONLINE 2</td>
<td>Panel TBC organised by TBC</td>
</tr>
<tr>
<td>11.00</td>
<td>ONLINE 3</td>
<td>Data Protection by Design and by Default in the Post-Covid World organised by IRI (Swedish Research Institute)</td>
</tr>
<tr>
<td>11.00</td>
<td>ONLINE 4</td>
<td>The role of OECD in Latin America: the dynamics of regulatory convergence in personal data protection organised by Data Privacy Brazil</td>
</tr>
<tr>
<td>12.00</td>
<td>ONLINE 1</td>
<td>Lunch</td>
</tr>
<tr>
<td>13.00</td>
<td>ONLINE 2</td>
<td>I spy with my little eye. Something beginning with... F. Intelligence agencies and fundamental rights organised by Privacy Platform (Renew Europe) [ENDS 14.15]</td>
</tr>
<tr>
<td>13.00</td>
<td>ONLINE 3</td>
<td>Global AI Governance: Perspectives from Four Continents organised by NCIS</td>
</tr>
<tr>
<td>13.00</td>
<td>ONLINE 4</td>
<td>Data Protection (R)Evolutions in the BRICS Countries organised by FGV</td>
</tr>
<tr>
<td>14.15</td>
<td>ONLINE 1</td>
<td>Political Panel on the EU Digital Strategy organised by CPDP</td>
</tr>
<tr>
<td>14.15</td>
<td>ONLINE 2</td>
<td>-panel TBC Closing the GDPR enforcement gap and looking at the enforcement model of the future organised by BEUC</td>
</tr>
<tr>
<td>14.15</td>
<td>ONLINE 3</td>
<td>Lunch</td>
</tr>
<tr>
<td>14.15</td>
<td>ONLINE 4</td>
<td>Lunch</td>
</tr>
<tr>
<td>15.30</td>
<td>ONLINE 1</td>
<td>Closing the GDPR enforcement gap and looking at the enforcement model of the future organised by BEUC</td>
</tr>
<tr>
<td>16.00</td>
<td>ONLINE 2</td>
<td>Connecting the dots: Privacy, data, racial justice organised by LSE</td>
</tr>
<tr>
<td>16.00</td>
<td>ONLINE 3</td>
<td>‘Rethinking ‘openness’ in the context of artificial intelligence” organised by CIPP M Bourne-mouth</td>
</tr>
<tr>
<td>16.00</td>
<td>ONLINE 4</td>
<td>How can data protection authorities’ supervision enforce compliance of major ICT service providers, including cloud service and communications providers? organised by TBC</td>
</tr>
<tr>
<td>17.15</td>
<td>ONLINE 1</td>
<td>ENFORCING RIGHTS IN A CHANGING WORLD</td>
</tr>
<tr>
<td>17.15</td>
<td>ONLINE 2</td>
<td>Towards Developing Comprehensive Privacy Controls that Minimizes Risks organised by UIUC USA</td>
</tr>
<tr>
<td>17.15</td>
<td>ONLINE 3</td>
<td>Technical standards bringing together data protection with telecommunication regulations, digital regulations and procurement organised by IEEE</td>
</tr>
<tr>
<td>17.15</td>
<td>ONLINE 4</td>
<td>Granular of holistic approach? Enforcing privacy rights in complex ICT ecosystems organised by PDP4E</td>
</tr>
<tr>
<td>18.30</td>
<td>ONLINE 1</td>
<td>Panel TBC organised by Twitter</td>
</tr>
<tr>
<td>18.30</td>
<td>ONLINE 2</td>
<td>Ready for a crisis: accelerated digitalization in education organised by VUB Data Protection on the Ground</td>
</tr>
<tr>
<td>18.30</td>
<td>ONLINE 3</td>
<td>Panel TBC organised by Twitter</td>
</tr>
<tr>
<td>18.30</td>
<td>ONLINE 4</td>
<td>Panel TBC organised by Twitter</td>
</tr>
</tbody>
</table>

Please note that this is a preliminary version of the programme.
<table>
<thead>
<tr>
<th>Time</th>
<th>Location</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.45</td>
<td>ONLINE 1</td>
<td>Closed Session: Privacy in Automated and Connected Vehicles organised by Secredas</td>
</tr>
<tr>
<td></td>
<td>ONLINE 2</td>
<td>Children's Rights in the Digital Environment: Risks, Opportunities, and Responsibilities organised by LIDERLAB</td>
</tr>
<tr>
<td></td>
<td>ONLINE 3</td>
<td>Panel TBC</td>
</tr>
<tr>
<td></td>
<td>ONLINE 4</td>
<td>Panel TBC</td>
</tr>
<tr>
<td>10.00</td>
<td></td>
<td>Coffee break</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Coffee break</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Coffee break</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Coffee break</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Coffee break</td>
</tr>
<tr>
<td>10.30</td>
<td></td>
<td>Closed Session: The Surveillance State: China and AI organised by Centre for AI and Digital Policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Standard for consent: still a dream or a soon-to-be reality? organised by INRIA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Securing personal data: the &quot;new&quot; normal organised by ENISA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Using health data in pandemics: the issues ahead organised by Panelfit</td>
</tr>
<tr>
<td>11.45</td>
<td></td>
<td>Shifting Responsibilities: The Challenges of Joint-Controllership organised by Facebook</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Emotional AI in Smart Cities organised by Chuo University</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Collateral Damages of Enforcement - Digital Services Act, Network Enforcement Act, and Loi Avia organised by PinG and DAV</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cybersecurity for Europe: Fostering rights through technology organised by Cybersec4Europe</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Exposure Notification During the COVID-19 Pandemic: reconciling fundamental rights and Public Health with legality attentive data science organised by LEADS/NIST</td>
</tr>
<tr>
<td>13.00</td>
<td></td>
<td>Lunch</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lunch</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lunch</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lunch</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lunch</td>
</tr>
<tr>
<td>14.15</td>
<td></td>
<td>Oversight and enforcement: Taking stock of design choices and trade-offs organised by Mozilla</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AI Audits: Black Box vs. White Box perspectives organised by Haifa University</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Algorithm-assisted decision-making in the public sector: Govern algorithms, while governing by algorithms organised by Microsoft</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Protecting Consumers in the Data Society: It's the Enforcement, Stupid! organised by Digital Clearinghouse</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dark by design: regulating manipulation in online environments organised by SnT</td>
</tr>
<tr>
<td>15.30</td>
<td></td>
<td>Coffee break</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Coffee break</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Coffee break</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Coffee break</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Coffee break</td>
</tr>
<tr>
<td>16.00</td>
<td></td>
<td>Panel on Data Sovereignty organised by Intel</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Automated decision-making: towards effective remedies in a changing world? organised by LCII</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Social media monitoring and movement tracking of political dissidents. The end of political asylum in the EU? organised by LSTS-DIGIACT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Where are the missing data subjects? Democratising data protection through participation organised by SPECTRE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Privacy, globalization and international data transfers: towards a new paradigm after Schrems II? organised by CEU San Pablo</td>
</tr>
<tr>
<td>17.15</td>
<td></td>
<td>Title TBC organised by Apple</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Artaccountability: Accountability, AI, and Art organised by Leiden University</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Violent Extremism, Vulnerability and the Limits of Confidentiality organised by VUB FRC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Multi-party data sharing and data subject rights: how to accelerate accountable data sharing? organised by CSLR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>An Expert Take on Schrems II - From the Experts from Schrems II organised by The Cordell Institute for Policy in Medicine &amp; Law (an Institute of Washington University in St. Louis)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>How can regulation help build trustworthy artificial Intelligence? organised by Workday</td>
</tr>
<tr>
<td></td>
<td></td>
<td>40 years of data protection and many more to come: Convention 108 and 108+ organised by Council of Europe</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Title TBC organised by Epic</td>
</tr>
<tr>
<td>19.45</td>
<td></td>
<td>EPIC, CNIL-INRIA Award</td>
</tr>
<tr>
<td>Time</td>
<td>Grande Halle</td>
<td>Online 1</td>
</tr>
<tr>
<td>-------</td>
<td>--------------</td>
<td>----------</td>
</tr>
<tr>
<td>8:45</td>
<td>Closed Session</td>
<td>Closed Session</td>
</tr>
<tr>
<td>10:00</td>
<td>Coffee break</td>
<td>Coffee break</td>
</tr>
<tr>
<td>10:30</td>
<td>Closed Session</td>
<td>AI &amp; humanitarian action: Raising the standards? organised by Brussels Privacy Hub</td>
</tr>
<tr>
<td>11:45</td>
<td>Panel TBC organised by TBC</td>
<td>Is ‘no’ still ‘no’ in an online world? Discussing non-consensual distribution of intimate images and deepfakes organised by Belgian Institute for the Equality of Women and Men</td>
</tr>
<tr>
<td>13:00</td>
<td>Lunch</td>
<td>Lunch</td>
</tr>
<tr>
<td>14:15</td>
<td>Automated Gender Attribution: It’s A Boy! It’s A Girl! Said the Algorithm organised by CPDP</td>
<td>AI Regulation in Europe &amp; Fundamental Rights organised by AI Ethicist</td>
</tr>
<tr>
<td>15:30</td>
<td>Coffee break</td>
<td>Coffee break</td>
</tr>
<tr>
<td>16:00</td>
<td>Data Governance Act: Data protection meets competition, IP rights, and innovation organised by Uber</td>
<td>Analysis of private communications in the fight against child sexual abuse online organised by KU Leuven</td>
</tr>
<tr>
<td>17:15</td>
<td>A Fireside Reunion: Data Protection at a Time of Uncertainty organised by IAPP</td>
<td>Artificial Intelligence and discrimination risks in the health sector organised by iHUB/Radboud University</td>
</tr>
<tr>
<td>18:30</td>
<td>Closing remarks by Wojciech Wiewiorowski</td>
<td></td>
</tr>
</tbody>
</table>
14:15 – POLITICAL PANEL ON THE EU DIGITAL STRATEGY

Organised by CPDP
Moderator TBC
Speakers Finn Myrstad, Norwegian Consumer Council (NO); Thomas Boué, BSA (BE); Karolina Mojewsowic, DG Just (EU); Mireille Hildebrandt, VUB (BE)

Coming soon

15:30 - Coffee Break

16:00 – E2EE: STUCK BETWEEN A ROCK AND A HARD PLACE

Organised by Microsoft
Moderator Christian Wiese Svanberg, Danish National Police (DK)
Speakers Scott Charney, Microsoft (UK); Susan Landau, Tufts University (US); Christine Runnegar, Internet Society (AI)

For more than two decades, the debate over End-to-End (E2E) Encryption has defied simple solution. The deployment of E2E encryption impacts a range of complementary and competing interests, including privacy, security, civil liberties, national security, public safety, and ICT innovation. While societies often seek policy solutions that balance such competing interests, encryption technology is, in a word, binary: E2E encryption is either breakable or it is not. As such, its use – or its restriction – will affect important societal values in ways both good and bad. And since governments often have different agencies and individuals addressing these values (e.g., privacy/data commissioners, law enforcement personnel), they may offer conflicting guidance on the way forward, thus highlighting the need for better communication and coordination between those interested in E2E encryption, including representatives from government, private companies, academia, and civil society.

This panel will frame and discuss the fundamental dilemmas this complex gives rise to.

- Encrypted devices and encrypted communications present different problems to law-enforcement investigations and different challenges in terms of ensuring security to the public. Of the most serious illegal activity that occurs online, do encrypted devices or encrypted communications present the greatest difficulty to law enforcement? What are the types of threats posed? What solutions do researchers and industry propose for enabling law-enforcement investigations?
- How do we ensure public safety, national security, and privacy when much of our economic, business, and social activity has moved online?
- Aside from access to encrypted communications and locked devices, what tools and techniques are needed by law enforcement agencies to conduct investigations in a digital world?
- How can we find a coordinated approach between lawmakers, companies, and academia to come up with an alternative to the “going dark debate” that serves all parties?

17:15 – ENHANCING PERSONAL DATA PROTECTION THROUGH DIGITAL SOVEREIGNTY

Organised by EDPS
Moderator Sjoerda Nas, Privacy Company (NL)
Speakers Thomas Zerdick, EDPS (EU); Stéphane Dumont, Gendarmerie Nationale (FR); Marco-Alexander Breit, German Federal Ministry for Economic Affairs and Energy (DE)

Digital sovereignty refers to Europe’s ability to make autonomous technological choices in the digital domain, while fostering digital innovation. The European Commission has identified digital policy as one of the key priorities of her 2019-2024 term and has stated that Europe must achieve ‘technological sovereignty’ in critical areas. The October 2020 European Council stressed that to be digitally sovereign, the EU must, inter alia, reinforce its ability to define its own rules, and to develop and deploy strategic digital capacities and infrastructure. One primary objective therefore is to ensure that the processing of personal data happens in line with EU values and privacy legislation, such as the General Data Protection Regulation (GDPR).
One such example, “Gaia-X” strives to set up a high-performance infrastructure for Europe, aiming at an open, digital ecosystem, which could allow (personal) data sharing in a secure and compliant manner. While Gaia-X could be a necessary element of EU industrial policy, additional actions may be necessary to create an EU technology policy, which follows neither a model of state controlled development, nor a model of market libertarianism.

- How is the progress and the public and private sector support for EU sovereign infrastructures such as Gaia-X?
- Which instruments do we need for Digital Sovereignty, e.g. in the domain of Software (EU Public License and other open source)?
- How can EU entities develop Insourcing strategies for innovation in the EU, e.g. by changing public procurement?
- How can Digital Sovereignty benefit privacy and protection of personal data?

11:45 – PANEL TBC

13:00 – I SPY WITH MY LITTLE EYE, SOMETHING BEGINNING WITH... F:
INTELLIGENCE AGENCIES AND FUNDAMENTAL RIGHTS

Organised by Privacy Platform (Renew Europe)
Moderator: Sophie in’t Veld, Member of European Parliament, Renew Europe (EU)
Speakers: Jan-Jaap Oerlemans, Utrecht University (NL); Edin Omanovic (UK); TBC

The activities of intelligence and security agencies are rapidly digitalising. New powers to analyse large amounts of data are being created, and every year, the pile of available information grows higher. Increasing cooperation and exchange between these agencies is necessary to keep Europe safe, but also has enormous consequences for our right to privacy and data protection. How can our rights and freedoms be reinforced, in balance with newly gained powers by these agencies? Scandal after scandal, we see that adequate supervision and enforcement is lacking. Which legal safeguards are supposed to protect us today, and which gaps are still existing and to be filled, and how? And how does Brexit affect our rights in intelligence cooperation?

14:15 – CLOSING THE GDPR ENFORCEMENT GAP AND LOOKING AT THE ENFORCEMENT MODEL OF THE FUTURE

Organised by BEUC
Moderator: Ursula Pachl, BEUC (BE)
Speakers: Gro Mette Møen, Forbrukerrådet (NO); Jean Gonié, Snap Inc; Gloria Gonzalez Fuster, VUB (BE); EDPB Representative (TBC)

The GDPR introduced an innovative enforcement system for tackling cross-border data protection infringements by establishing mechanisms for cooperation between DPAs and the consistent application of the rules across the EU. Over two years since it became applicable, the GDPR now risks becoming a “broken promise”. The one-stop-shop mechanism is showing its shortcomings and enforcement against Big Tech is uncertain. The expectations that the GDPR would tackle systemic data protection infringements inherent to the widespread commercial surveillance in our digital world have not materialised. All this is having a negative impact on the protection of millions of consumers across Europe. We are at a turning point. It is necessary to close this enforcement gap before it is too late. It is also necessary to draw lessons from this experience and start shaping the ideal enforcement model for the future.

- What is creating the GDPR enforcement gap and how can we address it?
- What are the problems with the one-stop-shop mechanism and how can we address them?
- What should be the ideal model for enforcement to protect consumers in the digital world?
- What model would ensure desired balance between EU-level and national enforcement structures, bridging the gap between the quintessential territoriality of enforcement and the cross-border nature of digital services?

15:30 – Coffee Break

16:00 – CONNECTING THE DOTS: PRIVACY, DATA, RACIAL JUSTICE

Organised by LSE
Moderator: Seda Gürses, TU Delft (NL)
Speakers: Yasminie Boudiaf, No Tech for Tyrants (UK); Sarah Chandler, European Digital Rights (BE); Nakeema Steffl-bauer, FrauenLoop (DE); Nani Jansen Reventlow, Digital Freedom Fund (DE)

Historically, privacy advocates and data protection professionals envision privacy as a universal right. In practice, however, there are deep inequities in how privacy gets enforced, who can safeguard their privacy, and what privacy means for different populations. These inequities raise the question of whether a universalist framework befits the lived experience of many subgroups, especially members of marginalized communities. In this provocative panel, we ask how an inclusive, collective vision of privacy look? A diverse group of practitioners, scholars, and advocates will put privacy and data protection in conversation with issues of racial injustice, migration control, and structural exclusion, exploring the exceptionalism, the

18:30 – CLOSED SESSION

19:45 – CPDP LATAM SIDE EVENT

CPDP2021 PANELS AT ONLINE 1

8:45 – CLOSED SESSION

10:00 - Coffee Break

10:30 – READY FOR THE NEXT “DIESELGATE” IN DATA PROTECTION: THE NEW REALITY OF COLLECTIVE REDRESS IN THE EU

Organised by Euroconsumers
Moderator: Marco Pierani, Euroconsumers (IT)
Speakers: Ursula Pachl, BEUC (BE); Marco Scialdone, Università Europea di Roma and InnoLawLab (IT); Bart Volders, ARCAS LAW (BE); Cornelia Kutterer, Microsoft (BE); Laura Somaini, winner My Data Is Mine Award

In 2020 the EU adopted a new law on collective redress which will allow citizens in all EU countries to go to court as a group if they have suffered the same damage, something consumer groups have been advocating for since more than 20 years. Data protection is one of the areas specifically covered in the new law. Consumer organisations have been pioneers in this area in those countries where collective redress was already allowed under national law, as demonstrated by the class actions launched in 2018 in Spain, Portugal, Italy and Belgium against Facebook. Now the possibility to claim collective redress for data protection damages becomes a reality across the EU. What does this mean for consumers? How will this new collective redress instrument be designed? And how will the compensation for a breach of privacy rights be defined?

- What are the main elements of the new EU directive on injunctions and collective redress?
- What are the possibilities and benefits it brings to consumers when it comes to the protection of their personal data and their privacy?
- What are the main challenges for collective redress in the area of data protection?
- What mechanisms can be envisaged to define the compensation for data protection damages?

11:45 – PANEL TBC

19:45 – CPDP LATAM SIDE EVENT

8:45 – CLOSED SESSION

10:00 - Coffee Break

10:30 – READY FOR THE NEXT “DIESELGATE” IN DATA PROTECTION: THE NEW REALITY OF COLLECTIVE REDRESS IN THE EU

Organised by Euroconsumers
Moderator: Marco Pierani, Euroconsumers (IT)
Speakers: Ursula Pachl, BEUC (BE); Marco Scialdone, Università Europea di Roma and InnoLawLab (IT); Bart Volders, ARCAS LAW (BE); Cornelia Kutterer, Microsoft (BE); Laura Somaini, winner My Data Is Mine Award

In 2020 the EU adopted a new law on collective redress which will allow citizens in all EU countries to go to court as a group if they have suffered the same damage, something consumer groups have been advocating for since more than 20 years. Data protection is one of the areas specifically covered in the new law. Consumer organisations have been pioneers in this area in those countries where collective redress was already allowed under national law, as demonstrated by the class actions launched in 2018 in Spain, Portugal, Italy and Belgium against Facebook. Now the possibility to claim collective redress for data protection damages becomes a reality across the EU. What does this mean for consumers? How will this new collective redress instrument be designed? And how will the compensation for a breach of privacy rights be defined?

- What are the main elements of the new EU directive on injunctions and collective redress?
- What are the possibilities and benefits it brings to consumers when it comes to the protection of their personal data and their privacy?
- What are the main challenges for collective redress in the area of data protection?
- What mechanisms can be envisaged to define the compensation for data protection damages?
WEDNESDAY 27 JAN 2021

17:15 – BORDERS AND BIOSURVEILLANCE: MIGRATION MANAGEMENT AND HIGH RISK TECHNOLOGICAL EXPERIMENTS IN THE TIME OF COVID-19

Organised by EDRi
Moderator Diego Narango, EDRi (BE)
Speakers Petra Molnar, Mozilla Fellow for EDRi (CA); Eleftherios Chelioudakis, Homo Digitalis (GR)

In the COVID-19 pandemic, technological innovations are enthusiastically presented as viable ways to stop the spread of the coronavirus. As governments move toward biosurveillance to contain the spread of the pandemic, we are seeing an increase in tracking, automated drones and other types of technologies that purport to help stop the spread of the virus and manage migration. However, if previous use of technology is any indication, refugees and people crossing borders will be disproportionately targeted. Virus-killing robots, cellphone tracking and artificially intelligent thermal cameras can all be used against people crossing borders, with far-reaching results and impacts on various human rights.

This panel will bring together the work of EDRi on borders and AI, actors like FRONTEX, and representatives of the community with lived experience of being targeted by technological experiments of pandemic surveillance.

18:30 – GRANULAR OF HOLISTIC APPROACH? ENFORCING PRIVACY RIGHTS IN COMPLEX ICT ECOSYSTEMS

Organised by PDP4E
Moderator Antonio Kung, PDP4E (FR)
Speakers Naomi Lefkovitz NIST (US); Member from PRISE team, KU Leuven (BE); Alejandra Ruiz TECNALIA (ES); EDP5 (BE)

ICT ecosystems are complex systems of devices, networks, backends operated and managed by multiple stakeholders. They are the backbone of infrastructures such as healthcare, smart manufacturing, transport, defense, energy, and others, which processes massive amounts of personal data. There is no convergence on how to ensure the enforcement of privacy rights in such complex systems. Most approaches are granular in that they focus on implementing privacy controls in every piece of the system, while others advocate for a more holistic approach to privacy (inter-organizational privacy) where all components share one common set of rules or principles or are based on interoperable frameworks or architectures. This panel aims at finding a solution to this debate, while covering aspects such as risk identification, governance, transparency, the engineering of control and protection capabilities, and the role of assurance to ensure trustworthiness.

• What does an inclusive, collective vision of privacy look like?
• How does race intersect privacy and data protection?
• What safeguards already exist against state surveillance for the protection of privacy?
• How do citizens become more aware of the use of AI in state surveillance in order to exercise their rights?

10:00 – Coffee Break

10:30 – PANEL TBC

11:45 – DATA PROTECTION BY DESIGN AND BY DEFAULT IN THE POST-COVID WORLD

Organised by The Swedish Law and Informatics Research Institute (IRI)
Moderator Liane Colonna, The Swedish Law and Informatics Research Institute (IRI), Stockholm University (SE)
Speakers Cecilia Magnusson Sjöberg, The Swedish Law and Informatics Research Institute (IRI), Stockholm University (SE); Athena Bourka, European Union Agency for Cybersecurity (ENISA) (EU); Veronica Buer, Norwegian Data Protection Authority (NO); Achim Klambude, Advisor to the Supervisor on Data Protection and Technology (EPDS) (EU)

Data Protection by Design and by Default (DPbDD) refers to the design and existence of embedded measures and safeguards and mechanisms that effectively protect the personal data protections principles, the rights and the freedoms of the data subject to data protection throughout the processing lifecycle of an application, service or product. In many ways, DPbDD can be seen as the sleeping giant of the GDPR: the entire burden of compliance hinges on this article where the data controller must design appropriate technological and organizational measures to address not just the core data protection principles listed in Article 5 but also the rights and the freedoms of the data subject and the requirements of the GDPR in general. This panel will consider the scope and enforcement of Article 25, particularly in the context of the pandemic and in the post-pandemic context. The discussion will cover issues including:

• What are the specific roles, responsibilities and liabilities of controllers, processors, hardware and software providers etc. when it comes to implementing this legal requirement?
• What does the concept of “the state of the art” mean and, who should be responsible for driving it?
• How should controllers demonstrate the effectiveness of a safeguard or measure?
• What is the relationship between AI and DPbDD?
14:15 – GLOBAL AI GOVERNANCE: PERSPECTIVES FROM FOUR CONTINENTS

Organised by: The Nordic Centre for Internet and Society (NCIS) at BI Norwegian Business School
Moderator: Samson Esayas, the Nordic Centre for Internet and Society (NCIS), BI Norwegian Business School (NO)
Speakers: Sofia Ranchordas, University of Groningen (NL); Amar Ashar, Harvard University (US); Angela Daly, University of Strathclyde (UK); Celina Bottino Beatriz, the Institute for Technology & Society of Rio de Janeiro (ITS Rio), Darcy Vargas Foundation, and the Children’s and Adolescent’s Rights Protection in Rio de Janeiro (BR)

The development and implementation of Artificial Intelligence (AI) within all domains of business, society, and governance has accelerated in recent years. Although current debate chiefly focuses on the economic consequences of AI, there is a growing awareness of the broader societal impacts of AI, especially the unequal ways in which the benefits and harms may be distributed across populations and geographies. This panel will bring perspectives from four continents on the societal impacts of AI, focusing on salient concerns and governance approaches in the respective regions. The aim is to leverage globally diverse viewpoints, and practical experience, and thereby contribute to the development of a shared understanding and more harmonized research efforts in addressing the societal impacts of AI technologies.

Salient features in the respective regions, both in terms of the concerns and the mechanisms for tackling them:
- What are the salient concerns and drivers of AI governance in your region?
- How has the policy response been so far?
- What effect is the COVID-19 pandemic having on the AI governance discourse? Has it intensified the urgency to deploy AI technologies as much as the need for regulatory responses?
- What do you think other regions can learn from the initiatives and responses in your region?
- Is it practical and desirable to think about global AI governance?

15:30 - Coffee Break

16:00 – RETHINKING ‘OPENNESS’ IN THE CONTEXT OF ARTIFICIAL INTELLIGENCE

Organised by: Centre for Intellectual Property Policy & Management (CIPPM) Bournemouth University
Moderator: TBC
Speakers: Maurizio Borghi, CIPPM (UK); Brigitte Vezina, CreativeCommons (NL); Javier Ruiz Diaz, Open Rights Group (US)

The development of algorithms requires access to large amounts of data.

Open Data initiatives address the need for access to data to help advance the development and adoption of beneficial AI in society.

The PSI Directive has helped to make data held by public sectors open for the use and training of AI systems which is not the case for privately held data specifically human-created works protected by copyright or neighbouring rights. More over, private companies who benefit from access to ‘open data’ are often in a position to create proprietary or quasi-proprietary entitlements around the outcomes of data processing, thereby turning open access into de facto exclusive rights in reverse.”

To address the challenges posed by and for AI access to data we may need to redefine what ‘openness’ means.

Following the introduction of an exception for text and data mining in the Directive on copyright in the Digital Single Market (2019/790), the proposed panel will discuss
- the dangers created by unregulated use of AI
- how the norm introduced by the new copyright directive can be used
- to mitigate such dangers and
- enable privately held data to become more accessible, allowing AI to flourish in ways that are beneficial to all stakeholders involved.

17:15 – AUGMENTED COMPLIANCE: THE CASE OF ALGORITHMIC IMPACT ASSESSMENT

Organised by: Augmented Law Institute - EDHEC Business School
Moderator: Björn Fasterling, EDHEC Augmented Law Institute (FR)
Speakers: Margot Kaminski, Colorado Law (US); Olivier Guillo, Smart Global; Henrik Junklewitz, European Commission (EU); Gianclaudio Malgieri, EDHEC Augmented Law Institute (FR)

The aim of the panel is to show how Data Protection by Design in the GDPR could encourage a holistic Algorithmic Impact Assessment under the GDPR, combining the DPIA requirements with the individual rights related to Automated Decision-Making. The panel wants to analyse what the concept of Algorithmic Impact Assessment is across different legislations and how different layers of automated decisions explanations might contribute to a dynamic DPIA of complex algorithmic data processing. The role of compliance software might also be pivotal in this process.

- How an Algorithmic Impact Assessment should look like across different Data Protection Legislations?
- Can Algorithmic DPIA and individual rights in the GDPR be connected in one only tool, as a disruptive and convenient compliance models for all data controllers?
- Can we imagine several layers of explanation of Automated Decision-Making under the GDPR?
- Can we “automate” compliance in case of algorithmic decisions?

18:30 – READY FOR A CRISIS: ACCELERATED DIGITALIZATION IN EDUCATION

Organised by: VUB Data Protection on the Ground
Moderator: Paul Timmers, European University Cyprus (CY)
Speakers: Alexandra Giannopoulou, University of Amsterdam (NL); Carrie Klein, Future of Privacy Forum (US); Michael Gallagher, University of Edinburgh (UK); Felix Seyfart, Berinför (CH)

A notable effect of corona-related confinement measures was the introduction of ‘emergency remote teaching’: educational processes had to be moved online in record time. While a plethora of tools was available, concerns about data protection and online safety arose instantly. Few educational organisations were ready to make a considered assessment of the reliability of options under pressure.

The education sector is in a constant state of flux. It is hard for many educational professionals to keep up with developments, especially technological advances. Recent years have also seen an interest in ‘revolutionizing’ education from the technology sector, promising to radically improve learning.

- What has the corona crisis done to (digital) education?
- How to evaluate EdTech platforms?
- Privacy as a form of power in schools
- What to expect? The future of Digital Education
Youth encounter both risks and opportunities online. In a rapidly evolving digital environment, efforts to defend youth privacy must delicately balance protecting and empowering youth online while allowing them to gradually develop resilience. This panel seeks to convene global youth, technology, and privacy experts to discuss existing and emerging global child privacy protection policies and strategies, key considerations for the public and private sectors, and the need to amplify youth voices in informing and shaping these policies.

- Why do youth warrant special privacy protections?
- How do youth feel about their privacy and what are their self-expressed needs and desires? How can youth voices be amplified in shaping youth privacy protections?
- How is youth privacy being protected globally? (Which ages should receive greater privacy protections, and should the parent or youth “own” those privacy rights? Should consent-based or rights-based legislation protection youth? Should youth privacy protections be included in comprehensive consumer privacy frameworks or are additional youth privacy policies necessary?)
- What youth privacy resources are available for youth, their families, and institutions working on their behalf?

**10:00 - Coffee Break**

**10:30 - PANEL TBC**

Coming soon

**11:45 - THE ROLE OF OECD IN LATIN AMERICA: THE DYNAMICS OF REGULATORY CONVERGENCE IN PERSONAL DATA PROTECTION**

Organised by Data Privacy Brasil
Moderator Bruno Bioni, Data Privacy Brasil (BR)
Speakers Giovanna Carloni, Centre for Information Policy Leadership/CIPL (UK); Carolina Botero, Fundación Karisma (CO); Maria Paz Canales, Derechos Digitales (CL); Miriam Wimmer, Ministerio da Ciência, Tecnologia, Inovações e Comunicações (BR); Elettra Ronchi, OECD (INT)

Historically, OECD has been a forum for the creation and dissemination of principles for the protection of personal data and there has been a convergence towards the implementation of these principles globally. The advancement of technology brings new legal and regulatory challenges, which are the subject of intense discussion within the OECD. So, in addition to the guidelines, today among its policy issues are privacy enforcement cooperation, digital identity and electronic authentication, cryptography, etc. As the global south catches up with Europe in terms of privacy and data protection regulation and as new countries are welcomed into the club, questions of how the OECD framework can (and should) shape its policies, as well as what precisely is OECD’s role in issues such as enforcement and mechanisms for transnational data flow, become pressing. This panel aims to cover these topics.

- What are some of the main points of the renewed agenda of the OECD in terms of personal data protection?
- What is the possible role of the OECD in facing the problem of data protection enforcement in the Global South?
- What is the scope of the OECD’s power in defining public policy in Latin American countries and how does that affect data protection in the region?
- What is the role of “soft power” and civil society in setting the agenda for data protection at the OECD?

**13:00 - Lunch Break**

**14:15 - DATA PROTECTION (R)EVOLUTIONS IN THE BRICS COUNTRIES**

Organised by FGV
Moderator Luca Belli, FGV-Rio Law School (BR)
Speakers Danilo Doneda, Public Law Institute (IDP) (BR); Wei Wang, University of Hong Kong (CN); Andrey Shcherbovich, Higher School of Economics, (RU); Smriti Parsheera, CyberBRICS project (IN)

The panel will explore tremendous evolutions that happened in the BRICS (Brazil, Russia, India, China, South Africa) data protection frameworks, over the past 12 months:

- the new Brazilian General Data Protection Law (LGPD) just entered in force and a new National Data Protection Authority (ANPD) will be established soon
- Russia is implementing data-intensive measures related to covid19 and a new Artificial Intelligence strategy
- India is finalising the new Data Protection Bill and is planning a new Data Empowerment and Protection Architecture (DEPA)
- China has just released its draft Personal Information Protection Law and plans a Global Initiative on Data Security
- Sections of the South African Protection of Personal Information Act (POPIA) entered in force. POPIA is now under “12-month grace period”
- How the enforcement Data Protection instruments in BRICS’s countries converge (or not)?
- Is data protection legal frameworks tied or even dependent in some level with cybersecurity frameworks?
- Which roles and institutional functions do the BRICS’ Data Protection Authorities (DPAs) play?
- Are there specific elements of resonance and harmonization among the data protection frameworks in BRICs’s countries?

**15:30 - Coffee Break**

**16:00 - DPA’S SUPERVISION AND COMPLIANCE OF ICT, CLOUD AND COMMUNICATIONS’ PROVIDERS**

Organised by EDPS
Moderator Wojciech Wiewiórowski, EDPS (EU)
Speakers Paul van den Berg, Dutch Ministry of Justice and Security (NL); TBC

EU controllers’ accountability includes the creation design of compliant processing systems, e.g. by observing data protection by design and by default. In practice, public authorities in the EU are using the systems and applications provided by large companies, often with built-in tracking and data collection features, based on the companies’ standards, frequently unilateral terms and conditions. Some argue that the available technology limits their capability to achieve data protection compliance and that terms and conditions cannot be adapted to specific processing operations.

In line with its 2020-2024 strategy, the EDPS concluded an investigation on widely used office automation tools by the EU institutions. Findings and recommendations on the use of Microsoft products and services by EU institutions are likely to be of interest to all public authorities in EU/EEA Member States. This concrete case helps to assess the EDPS’ strategic objective, like that of other DPAs, to ensure that public administrations in their contractual relationships with ICT service providers use terms that reinforce the public administrations’ control over how and for which purpose personal data is processed.

- How can DPAs use their enforcement powers through supervision of public authorities to influence the data protection compliance of ICT service providers, including cloud service and communications providers?
What is the role of ICT providers with regard to public administrations and how do their practices affect consumers and clients of public authorities?

How should public authorities shape their contractual and business relationships with service providers and systems developers in order to improve data protection compliance?

What should be a controller-processor contract in terms of form and content and how could it guarantee that controllers keep control and ensure fair and lawful processing of personal data of citizens?

To what extent can the right to the protection of personal data be interfered with by these technologies and how could these technologies be unchallengeable, due to their proprietary nature and/or unintelligible decision-making.

What role can the rights to data portability and interoperability play in the data economy and what are the limits?

What is the role of ICT providers with regard to public administrations and how do their practices affect consumers and clients of public authorities?

What is the state-of-the-art of these technologies in terms of regulation, practice and performance and how prepared is the world should expect next.

What prompted the seismic shift towards privacy protection in the US?

What is the role of the EU legislator in this debate? Is an EU-wide legislative solution necessary? What issues should be covered by such new legal instrument (e.g. the material and personal scope of application – serious crime only, new types of service providers, etc.)? How would such legislative initiative relate to other ongoing reforms (e.g. e-evidence and e-privacy)?

What are the risks of not having a solid legal framework on data retention at national and EU level?

What role can the rights to data portability and interoperability play in the data economy and what are the limits?

What is the role of the EU legislator in this debate? Is an EU-wide legislative solution necessary? What issues should be covered by such new legal instrument (e.g. the material and personal scope of application – serious crime only, new types of service providers, etc.)? How would such legislative initiative relate to other ongoing reforms (e.g. e-evidence and e-privacy)?

What are the risks of not having a solid legal framework on data retention at national and EU level?

What role can the rights to data portability and interoperability play in the data economy and what are the limits?

What is the role of the EU legislator in this debate? Is an EU-wide legislative solution necessary? What issues should be covered by such new legal instrument (e.g. the material and personal scope of application – serious crime only, new types of service providers, etc.)? How would such legislative initiative relate to other ongoing reforms (e.g. e-evidence and e-privacy)?

What are the risks of not having a solid legal framework on data retention at national and EU level?
How can rights and standards enable SMEs to compete with incumbent platforms and what are the right economic incentives to build the necessary digital infrastructure?

What can the Digital Services Act and the Data Act do to make portability and interoperability rights truly effective?

13:00 – Lunch Break

14:15 – CIVILIAN OVERSIGHT FOR THE USE OF SURVEILLANCE TECHNOLOGY

Organised by VUB Chair in Surveillance Studies
Moderator Rosanne de Velde, Vrije Universiteit Brussel (BE)
Speakers Plato, Markaz University (UK); Quirine Eijkman, College voor de Rechten van de Mens (NL); TBC

The VUB Chair in Surveillance Studies panel aims to bring together members of different parts of society to think about citizen participation and civilian oversight for the implementation of intrusive surveillance technologies. Aiming to foster an environment of exchange of ideas and learning opportunities from abroad, our panel is made up of a civil liberties representative, an academic expert, an expert/experienced member of citizen oversight mechanisms in the US, and a member of a Belgian oversight body with no citizen involvement.

• Pros and cons: why (or why not) consider civilian oversight?
• Under what conditions is civilian oversight preferred?
• How does it relate to traditional mechanisms of oversight?
• Can we learn something from a US perspective?

15:30 – Coffee Break

16:00 – TOWARDS DEVELOPING COMPREHENSIVE PRIVACY CONTROLS THAT MINIMIZES RISKS

Organised by UIUC (US)
Moderator TBC
Speakers Masooda Bashir, UIUC (US); Lisa Bobbitt, CISCO Corp (US); Guy Cohen, Privitar Corp (UK); Zee Kin, Deputy Commissioner at Personal Data Protection (SG)

Advancement of technologies has created new threat landscapes in the Privacy/Security domains. Therefore, information privacy protections have become a vital element for all computing environments. We can no longer presume that information privacy refers only to the confidentiality of personal information, but rather it is to include the protection of personal information and safeguarding of the collection, access, use, dissemination, and storage of personal and sensitive information. One approach to ensure privacy preserving environments is to minimize privacy risks. To achieve this goal, we propose the development of a comprehensive set of privacy criteria and controls that can serve as the framework for privacy researchers, practitioners, and auditors as well any organization. We call this framework the Comprehensive Criteria for Privacy Protection (C2P2) and the proposed panel will present and discuss this newly developed framework and provide their perspective.

• What is the Comprehensive Criteria for Privacy Protection (C2P2) framework and which are its related opportunities and challenges?
• How can controls, such as C2P2, be systematically engineered into cloud-based products, services, and enterprise applications?
• Considering technical and legal challenges, how is it possible to design comprehensive privacy risk management strategies by which personal data can be used safely while building users’ trust and mitigating privacy regulatory risks?
• Which are the perspectives on the development of a risk-based certification for Singapore’s data protection standards that addresses APEC cross border privacy rules and privacy recognition for processors systems?

17:15 – TECHNICAL STANDARDS BRINGING TOGETHER DATA PROTECTION WITH TELECOMMUNICATIONS REGULATION, DIGITAL REGULATIONS AND PROCUREMENT

Organised by IEEE
Moderator Rob van Eijk, Future of Privacy Forum (NL)
Speakers Paul Nemitz, European Commission (EU); Mikulas Pecka, European Parliament (EU); Amelia Andersdotter, IEEE 802.11 (SE); Clara Nappel, IEEE (AT); Francesca Bria, Self (IT)

Since the European Union passed the GDPR, data protection is a key component of the Union’s strategies in areas ranging from citizenship policies to industrial policy. Ensuring the systematic application of data protection principles across many policy areas is, however, a difficult task with many policy areas lagging behind or sometimes outright contradicting this fundamental rights goal. Technical standards can and do play a role in bridging these gaps, and since the entry into force of the GDPR there have, in fact, been major advances from the most fundamental infrastructural levels of network infrastructure to the end-consumer oriented interfaces that incorporate privacy leadership. This panel will deal with the challenges of ensuring that privacy-enhancing technical standards are developed in different parts of the European policy-making machinery.

• Is the GDPR providing moral leadership?
• How does this leadership manifest in privacy-enhancing technologies? How can the EU absorb industry-developed standards that incorporate privacy considerations?
• In which ways can we ensure cooperation across policy areas (procurement, consumer, data protection, communications)?
THURSDAY 28th JANUARY 2021

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

CPDP2021 PANELS AT GRANDE HALLE

8:45 - CLOSED SESSION

10:00 - Coffee Break

10:30 - CLOSED SESSION

11:45 - SHIFTING RESPONSIBILITIES: THE CHALLENGES OF JOINT-CONTROLLERSHIP

Organised by Facebook
Moderator Valentina Colcelli, Italian National Research Council (IT)
Speakers Nana Botchorichvili, CNIL (FR); Michele Finck, Senior Research Fellow at Max Planck Institute (DE); Diletta Di Cicco, Steptoe (IT/BE); Cecilia Alvarez, Facebook (ES)

With their guidelines on the concepts of controller, processor and joint-controllership, and the one on targeting of social media users, the EDPB has shown the desire to provide guidance about the allocation of data protection responsibilities. This gives rise to new complications and questions.

- What new proposals on the construction of joint-controllership are on the table?
- What are the merits and challenges of a joint liability for different actors?
- Which sectors will be impacted?
- How to navigate the challenges of joint-controllership?

13:00 - Lunch Break

14:15 - OVERSIGHT AND ENFORCEMENT: TAKING STOCK OF DESIGN CHOICES AND TRADE-OFFS ORGANISED

Organised by Mozilla
Moderator Jennifer Baker, EU technology journalist (BE)
Speakers Alice Munyua, Mozilla Corporation (US/KG); Benoît Loutrel, Science Po Paris (FR); Willem Debeuckelaere, Former President, Belgium Privacy Commission (BE); Shinnini Kumar, Former Head, Consumer Banking, Citi Bank India (IN)

Questions of oversight and enforcement are at the fore in several domains of digital policy. Existing legislative frameworks within the data protection sphere tend to include comprehensive oversight structures, while contemporary debates concerning content regulation and competition in digital markets are heavily occupied with the potential role of new oversight and enforcement mechanisms.

This panel discussion will comparatively assess issues around oversight and enforcement, drawing from experience from within and without the tech sector. In doing so, it will provide guidance for policymakers and policy stakeholders on the necessary conditions for effective oversight and enforcement in existing and future regulatory frameworks.

- What has worked and what has not worked in terms of the oversight and enforcement structures of the GDPR?
- What insights should tech policy regulators learn from this when considering the governance set-up for other policy issues (e.g. online content)?
- What resources and powers to regulators in the tech sector require to execute their mandate in respective domains?
- What can we learn about oversight and enforcement from other sectors that have a long tradition of agency-led regulation (e.g. financial services)?

15:30 - Coffee Break

16:00 - PANEL ON DATA SOVEREIGNTY

Organised by Intel
Moderator Riccardo Masucci, Intel (BE)
Speakers Meenakshi Lekhi, Lok Sabha (IN); Audrey Plonk, OECD (INT); Samm Sacks, New America (US)

Data sovereignty approaches are becoming more prominent worldwide. Drivers are multiple: privacy concerns and law enforcement access to data - as shown in the Schrems II ruling in Europe or the Tik Tok/We Chat bans in the US - as well as the creation of competitive advantages for national digital champions. Countries like India and China are developing their personal and non-personal data policy and governance frameworks. Data localization requirements are spreading across regions, new forms of data sharing and the establishment of local data repositories are currently under discussion: all these will increasingly affect global data flows and the ability for organizations to access data to develop and deploy new technologies like artificial intelligence and autonomous driving. The panel will assess current and future trends around data sovereignty, data access and flows to outline some public policy priorities and solutions.

- Is data localization the answer to privacy and national security concerns?
- Would more “data sovereign” countries be also more competitive?
- How can global interoperability and harmonization be ensured?
- How will these trends in global data flows affect the adoption of autonomous technologies?

17:15 - TITLE TBC

Organised by Apple
Moderator TBC
Speakers TBC

Coming soon

18:30 - RIGHTS IN THE DIGITAL WORLD: HOW TECHNOLOGY SUPPORTS DATA PROTECTION THROUGH INNOVATIVE PRIVACY PRESERVING TECHNOLOGIES

Organised by Google
Moderator TBC
Speakers TBC

As technology evolves in the digital world, privacy and data protection should be at the core of these developments. Different and innovative ways technologies can do more with less data is one key topic the industry has been discussing and investing resources.
This panel will discuss recent technological advances in differential privacy, federated learning, homomorphic encryption, and anonymization and how they fit into existing regulatory schemes, and the challenges and tradeoffs involved. It will also talk through how these new technologies support user’s right to privacy and how the academia, civil society, private and public sector can collaborate on these developments.
• Is the right not to be subject to automated decision-making in Art. 22 GDPR sufficient to ensure fundamental rights protection?
• Beyond the GDPR, does automated decision-making require the introduction of new or modified remedies under EU law?
• Could the EU develop a more streamlined remedial approach instead of a sector-specific one?
• Should the non-contractual liability remedy be modified in light of automated decision-making risks?

17:15 - ARTACCOUNTABILITY: ACCOUNTABILITY, AI, AND ART
Organised by Leiden University
Moderator: Eduard Fosch-Villaronga, Leiden University (NL)
Speakers: Peter Booth, BI Norwegian Business School (NO); Lucas Evers, WAAG Foundation (NL); Fiona McDermott, University of Dublin (IE); Piera Riccio, Oslo Metropolitan University (NO); MetaLAB at Harvard (US); Vincent Rioux, National Superior School of Fine Arts (FR)

This panel combines perspectives on Art, Society, & Technology. In particular, it focuses on artistic perspectives on algorithmic accountability. The panel starts with an overview of how the Arts play an essential role in intervening in critical social issues, such as labor politics, privacy, and education. The panel will then draw our attention to a specific case scenario, i.e., urban algorithmic accountability. We will learn about the digitization of cities and how municipal data professionals can give testimony of algorithmic-based decisions that affect citizens. The panel closes with some artistic perspectives on transparency and the role that education plays in stressing the importance of being accountable in an increasingly algorithmic society. The panel discussion will be divided into three clusters: (1) the Interplay of Art, Society and Technology, (2) Algorithmic Accountability and Art, and (3) Art, Education, and Responsibility.

• The Interplay of Art, Society and Technology
• Algorithmic Accountability and Art
• Art, Education, and Responsibility

18:30 – HOW CAN REGULATION HELP BUILD TRUSTWORTHY ARTIFICIAL INTELLIGENCE?
Organised by Workday
Moderator: Audrey Plonk, OECD (INT)
Speakers: Barbara Cosgrove, Workday (US); Daniel Braun, Deputy Head of Cabinet, Vice President Vera Jourova (BE)

Public policy on Artificial Intelligence is progressing in Europe, and around the world. The European Commission is expected to publish draft legislation this spring. The Commission has set out its dual objectives of creating an AI ecosystem of trust and enforcing rights in a changing world.

• Should the non-contractual liability remedy be modified in light of automated decision-making risks?
• Beyond the GDPR, does automated decision-making require the introduction of new or modified remedies under EU law?
• Could the EU develop a more streamlined remedial approach instead of a sector-specific one?
• Should the non-contractual liability remedy be modified in light of automated decision-making risks?

CPDP2021 PANELS AT ONLINE 2

8:45 - CHILDREN’S RIGHTS IN THE DIGITAL ENVIRONMENT: RISKS, OPPORTUNITIES, AND RESPONSIBILITIES
Organised by LIDER LAB, Scuola Superiore Sant’Anna
Moderator: Denise Amram, Scuola Superiore Sant’Anna (IT)
Speakers: Ruggero G. Pensà, University of Turin (IT); Jordi Albo-Canals, Dyna Tech 2012 (ES); Juan Marínez Otero, iCmedia (ES); Katharina Kaeling, University of Bonn (DE)

IoT services develop new forms of free expression, organisation and association, providing unprecedented access to information and ideas, addressing political, economic, and social trends.

This panel focuses on children as vulnerable users. Access to IoT contributes to the promotion of children’s well-being (essential for education purposes during the pandemic), but it also intensifies existing inequalities (digital divide for cultural and economic differences) and risks (fake news, cyberbullying, monitoring and profiling AI-based toys/applications, sexting, grooming).

Data protection and privacy-preserving shall be boosted in terms of i) technical safety for service providers/developers, ii) parents, caregivers, institutions (starting from Schools) awareness and responsibilities, iii) skills, access, and education for children, iv) inclusion and equality.

The panel promotes a roadmap for the best interests of the child in the IoT, discussing best practices, measures to enhance rights and mitigate risks in the digital environment.

• Enhancing equal access to information society; from education needs to a cultural evolution, boosting inclusion and non-discrimination;
• Facing digital divide and promoting awareness for risks & opportunities in the information society: best interests of the child in the IoT;
• Enhancing privacy and data protection within social networks, AI-based toys, IoT App: boundaries for parental responsibilities, institutions, and services’ providers and developers;
• Digital skills and competence for new educational and learning path.

10:00 - Coffee Break

10:30 – STANDARD FOR CONSENT: STILL A DREAM OR A SOON-TO-BE REALITY?
Organised by INRIA
Moderator: Nataliia Bielova, INRIA (FR)
Speakers: Armand Heslot, CNIL (FR); Cristiana Santos, University of Utrecht (NL); Romain Robert, NOYB (AT); Aurelie Pol, Mind Your Privacy (ES); Cristina Santos, University of Utrecht (NL); Benoit Oberlé, Sirdata (FR)

While users surf the Web, trackers collect their data for purposes that often require consent, according to Article 5(3) of the ePrivacy Directive. The amount of website audits, complaints and regulatory enforcement actions on consent - both from DPAs and the Court of Justice - have substantially increased. However, all these actions depend on complex manual analysis of websites that includes detection of a tracking technology; identification of a purpose of each tracking technology; analysis whether consent is required; evaluation of consent validity.

Recent guidelines by the EDPB and DPAs clarify and strengthen the rules for consent requirements and propose best practices, but the implementation of consent on websites still diverges. The panel is going to discuss the following questions:
• Can transparency, with regard to AI decision-making, affect public perceptions on the legitimacy of AI decisions and the role that technology companies can play in ensuring that AI is developed responsibly?

• What is the responsibility of governments when deploying algorithm-assisted decision-making tools?

11:45 - COLLATERAL DAMAGES OF ENFORCEMENT - DIGITAL SERVICES ACT, NETWORK ENFORCEMENT ACT, AND LOI AVIA

Organised by: Privacy in Germany (PinG) / Deutscher Anwaltsverein (DAV)
Moderator: Niko Harting, Pinto (DE)
Speakers: Anupam Chander, Georgetown University (US); Arnd Haller, Google (DE); Bojana Bellamy, Hunton Andrews Kurth LLP (UK); Suzanne Vergnolle, Université Paris II Panthéon Assas (FR); Tieno Wolken, European Parliament (EU)

In the past years, member states like Germany (Network Enforcement Act) and France (Loi Avia) have passed laws containing new obligations for social media providers to protect and enforce rights in the digital sphere. This controversy legislation (the Loi Avia has been declared partly unconstitutional) is about to be amended on the national and EU level. The EU Digital Service Act is supposed to set new rules for the liability of intermediaries and improve enforcement.

While it seems hard to argue with the goals of fighting hate speech, fake news and the spread of conspiracy ideologies, this legislation has some serious side effects: Overblocking, blurred lines between public and private tasks, and—of course—data protection issues concerning social media users. This panel will discuss experiences with national legislation and possible “collateral damages” of the new European approach.

• How will the EU Digital Service Act change the role of intermediaries?
• How will it help to improve the enforcement of laws in the digital sphere?
• What side effects might it bring for free speech, data protection, and other goods?
• How does the Digital Service Act relate to similar national legislation?

13:00 – Lunch Break

14:15 – ALGORITHM-ASSISTED DECISION-MAKING IN THE PUBLIC SECTOR: GOVERN ALGORITHMS, WHILE GOVERNING BY ALGORITHMS

Organised by: Microsoft
Moderator: TBC
Speakers: Matthias Spielkamp, AlgorithmWatch (DE); Cornelia Kutterer, Microsoft (BE); Ger Baron, City of Amsterdam (NL); Jennifer Cobbe, University of Cambridge (UK)

Governments and authorities across Europe increasingly deploy automated decision-making systems and AI-powered data analysis to provide ‘better public services’. Yet, this development has met with parallel concerns over negative and unfair outcomes for citizens, or potentially denial of consequential services altogether. This panel will discuss strategies to achieve transparent and accountable systems and mitigate these risks, both during development and deployment of Algorithm-assisted decision-making systems. The discussion will shed light on current approaches to responsible AI, including through practices, tools, standards and legislation.

• What is the role that technology companies can play in ensuring that AI is developed responsibly?
• What is the responsibility of governments when deploying algorithm-assisted decision-making tools?
• Can transparency, with regard to AI decision-making, affect public perceptions on the legitimacy of AI decisions and decision-makers?
• How can we provide transparency on algorithms in a way that it will be understood by citizens?

15:00 – Coffee Break

16:00 – SOCIAL MEDIA MONITORING AND MOVEMENT TRACKING OF POLITICAL DISSIDENTS. THE END OF POLITICAL ASYLUM IN THE EU?

Organised by: LSTS (DIGIACT Project), VUB
Moderator: Marcus Michaelsen, LSTS, VUB (BE)
Speakers: Sibel Top, FRC; VUB (BE); Christoph Marchand, Juscogents (BE); Petra Molnar, York University Toronto (CA); Botagoz Jardemalie, Human rights defender, Licensed Attorney in the State of New York (US)

The session deals with current challenges to the right to political asylum in the European Union, both from within and beyond its borders. Exiled dissidents who have taken refuge in the EU are threatened with different tactics of transnational repression. Illiberal regimes use digital surveillance, online attacks as well as extradition requests and Interpol red notices to target political emigrants outside their territory. But the EU itself also exercises extraterritorial power against asylum seekers: migrants are subject to social media monitoring, movement tracking and other forms of border management before they even enter European territory. And finally, internal dissidents lack political protection too, as illustrated by the cases of whistleblowers and separatist movements. From different angles, the panel highlights the pressures on fundamental human rights in the 21st Century, resulting from the impacts of globalization and digitalization.

• How is the right to political asylum in the EU currently challenged and undermined?
• What are the EU governments’ legal obligations in protecting political refugees on their territory?
• What role do digital technologies play in threats against the human rights of political refugees?
• How to protect and strengthen asylum seekers against digitally enabled threats to their rights?

17:15 – VIOLENT EXTREMISM, VULNERABILITY AND THE LIMITS OF CONFIDENTIALITY

Organised by: Fundamental Rights Research Centre, Vrije Universiteit Brussel / FRC, VUB
Moderator: Carlotta Rigotti, Fundamental Rights Research Centre, Vrije Universiteit Brussel (BE)
Speakers: Harald Weilnböck, Bundesministerium für Inneres (AT); Jedrzej Niklas, School of Journalism, Media and Culture, Cardiff University (UK); Schielan Babat, Türkische Gemeinde in Schleswig-Holstein e.V./PROvention (DE); Nőr Nói Loidein, Institute of Advanced Legal Studies, University of London (IALS) (UK)

Exit counselling means to facilitate deradicalisation and personal growth, so that clients distance themselves from anti-democratic and violent-extremist thinking and behaviour. Exit counselling therefore implies intensive work with most sensitive personal and family/community issues – sometimes resembling psychotherapy; it thus requires voluntary participation, confidentiality and the processing of personally-identifiable data. Yet, by working in an inter-agency scenario, exit practitioners are often asked to report and/or give risk-assessments about clients. Besides, data protection issues around exit programs are often misunderstood as conflict between individual rights and state security interests, with the consequence of disregarding the vulnerability of both the clients and democracy itself and its quintessential separation of powers/functions. Although the GDPR does not explicitly define vulnerable data subjects, clients should be protected because of the higher risks of damages arising to data processing and/or to the outcomes of such processing.

• How to define vulnerable data subjects in exit counseling, within the data protection framework?
• How is the right to data protection of clients ensured in the inter-agency setting of exit programs?
• To what extent is the professional secrecy of exit practitioners limited by security concerns, having special regard to the right not to testify in court?
• Are there alternatives to further balance the vulnerability of clients and the professional secrecy of exit workers against security concerns?
THURSDAY 28 JAN 2021

18:30 – 40 YEARS OF DATA PROTECTION AND MANY MORE TO COME: CONVENTION 108 AND 108+

Organised by Council of Europe
Moderator Vincent Manancourt, Politico (BE)
Speakers Joseph A. Cannataci, Special Rapporteur on the Right to Privacy (INT); Fanny Hildegi, Access Now (BE); Ulrich Kelber, Federal Commissioner for Data Protection and Freedom of Information (DE); Sophie int’ Veld, Member of the European Parliament (EU)

Data protection day marks an important celebration this year. The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (more commonly known as “Convention 108”) celebrates its 40th anniversary. 40 years later, it counts 55 Parties from Africa, Latin-America and Europe, and is still the only legally binding multilateral instrument on the protection of privacy and personal data open to any country in the world.

Looking back at those 40 years, the normative developments deriving from Convention 108 are immense and need to be acknowledged. Looking ahead, this landmark instrument has recently been modernised to better match the new realities of an increasingly connected world and to strengthen its effective implementation. The Convention aimed at delivering two essential objectives: facilitating data flows and respecting human rights and fundamental freedoms, including human integrity and dignity. Has it lived up to its promises and what is its role at global level in the digital age?

- The Modus operandi of data protection in Convention 108
- Convention 108: utopist vision or achieved objective?
- An element of response to the contemporary transborder data flows dialectic?
- 108+: cosmetic or functional?

CPDP2021 PANELS AT ONLINE 3

8:45 - PANEL TBC

Coming soon

10:00 – Coffee Break

10:30 – SECURING PERSONAL DATA: THE “NEW” NORMAL

Organised by ENISA
Moderator Prokopios Drokgaris, ENISA (EU)
Speakers Rosa Barcelo, Squire Patton Boggs (BE); Cédric Lauradoux, INRIA (FR); Zoi Kardasiadou, DG Justice (FR); Fabian Praßer, Charité – Universitätsmedizin Berlin (DE); Peter Kraus, EDPB (EU)

The Covid-19 pandemic has changed our everyday habits in several ways, bringing digital communication into the front line and new processes that require the processing of our personal data. The wide adoption of online videoconferencing tools, both for professional and personal reasons, is one prominent example of this change. Contact tracing apps is another example of the so-called “new normal”, being considered by several EU Member States as an appealing option to support public health against the pandemic spread. While clearly beneficial, there are often serious questions raised over the security and privacy of this new mode of operation and related applications. Both Member State authorities, EU bodies and EU commission have issued a number of guidance documents on the considerations that should be taken into account, e.g. on the security of online communication tools or the contact tracing apps.

- In what ways has the “new” normal affected the existing considerations related to security of personal data processing?
- What are the key strengths and the new challenges we face when considering security of personal data?
- How can Privacy Enhancing Technologies support this transition? How can end users (Data subjects) be better prepared and how can they protect themselves?

11:45 – CYBERSECURITY FOR EUROPE: FOSTERING RIGHTS THROUGH TECHNOLOGY

Organised by CyberSec4Europe - Trust in Digital Life
Moderator Athena Bourka, ENISA (EU)
Speakers Alessandro Manteleiro, Polytechnic University of Turin (IT); Giuseppe Vaciago, R&P Legal, University of Insubria (IT); Vanesa Gil Laredo, BBVA (ES); Marko Hölbl, University of Maribor (SI)

The recent global pandemic experience has confirmed the key role of IT Infrastructures and digital services in our societies. It has also shown the fragile nature of digital ecosystems when not based on responsible and common cybersecurity strategies. This is even more important in the context of European interoperable services and critical infrastructures.

Against this background, this panel deals with data security and cybersecurity from a business perspective, focusing on relevant legal provisions and linking them to technological and organizational measures supporting their implementation. This will reveal interconnections between legal instruments and the technology-focused backbone of the EU approach in this field. The panel will identify the key elements of the different regulations that are crucial for data security and contribute to define a framework based on five main pillars: risk-based approach, by-design approach, reporting obligations, resilience, and certification schemes.

- How can the legal framework on data protection and data security provide a favourable environment for the development of harmonised data security policies and strategies?
- How can the interconnection between different legal framework (GDPR, NIS, PSD2 e eIDAS) stimulate best practices and legal tech tool to facilitate integrated compliance with similar obligations (i.e. reporting, risk assessment and security measures)?
- What are the main elements to consider when designing and implementing an information security management strategy, based on regulatory requirements and security standards and with the aim of guaranteeing operational resilience of the organisation?
- Which new technologies are the most important to meet the requirements of EU cybersecurity and data security regulations?

13:00 – Lunch Break

14:15 – PROTECTING CONSUMERS IN THE DATA SOCIETY: IT’S THE ENFORCEMENT, STUPID!

Organised by Digital Clearing House
Moderator Alexandre de Street, University of Namur (BE)
Speakers Andreas Mündt, German Bundeskartellamt (DE); Marie-Laure Denis, CNIL (FR); William Kovacic, George Washington University Law School and former chairman of the US Federal Trade Commission (US); TBC

Discussions about the protection of individuals in the digital era often focus on whether the rules are adequate. However, experience from the Digital Clearinghouse shows that effective enforcement is at least as important as the substance of the rules and yet sometimes neglected in the policy debate.

The panel looks back at recent key enforcement actions that aimed to improve the effectiveness of consumer rights, including the Facebook decision of the Bundeskartellamt and the Google decision of the CNIL. Lessons are drawn for optimizing the institutional set-up for enforcement and collaboration between authorities.

15:15 – Technologies and Security: Protecting the Nimble

Organised by ENISA
Moderator Prokopios Drokgaris, ENISA (EU)
Speakers Francesco Buscemi, Sapienza University of Rome (IT); Frédéric Bouquet, University of Nantes (FR); Alessandro Mantelero, Polytechnic University of Turin (IT); Giuseppe Vaciago, R&P Legal, University of Insubria (IT); Vanesa Gil Laredo, BBVA (ES); Marko Hobl, University of Maribor (SI)

- How can the interconnection between different legal framework (GDPR, NIS, PSD2 e eIDAS) stimulate best practices and legal tech tool to facilitate integrated compliance with similar obligations (i.e. reporting, risk assessment and security measures)?
- Which new technologies are the most important to meet the requirements of EU cybersecurity and data security regulations?
What lessons can be drawn from recent cases at the national level to improve the enforcement of consumer rights in the areas of data protection, competition and consumer law?

What modes of cooperation between different regulatory authorities should be further developed?

Is there a need for more focused enforcement where cases are prioritized and assessed in accordance with the impact of the practices under investigation?

Should the future Digital Services Act establish an equivalent in Europe of the US Federal Trade Commission?

15:30 - Coffee Break

16:00 - WHERE ARE THE MISSING DATA SUBJECTS? DEMOCRATISING DATA PROTECTION THROUGH PARTICIPATION

Organised by SPECTRE Project
Moderator: Athena Christofi, SPECTRE project (BE)
Speakers: Mihalis Kritikos, STOA/EPRES - European Parliament (EU); Max von Grafenstein, Einstein Center Digital Future, University of the Arts (DE); Roos Groothuizen, Independent Media Artist and Designer (NL)

EU data protection law wants to empower individuals through consent and data subject rights. Yet, in practice, crucial decisions like the assessment of risks and the balancing of interests at stake, features of GDPR’s risk-based approach, are fully entrusted to controllers. Individuals, as data subjects and citizens of an increasingly datafied society, have little influence on desirability, necessity, proportionality and design of a processing operation. In an era where ubiquitous computing - by private and public data controllers - brings out profound changes in the enjoyment of fundamental rights, but also to the economy and society, this panel discusses public participation in DPIAs as a tool for ex-ante control, legitimisation and democratisation of data protection. In other risk-based frameworks (e.g. Technology Assessments), opening up to the public is agreed to be highly desirable, and in some instances even clearly legislated.

- Is there an obligation to engage individuals in DPIAs under the GDPR?
- Stakeholder participation in DPIAs can contribute to enforcing the right to data protection but why is no one doing it?
- Who to engage and how?
- Technocracy vs societal input and legitimization: irreconcilable values?

17:15 - MULTI-PARTY DATA SHARING AND DATA SUBJECT RIGHTS: HOW TO ACCELERATE ACCOUNTABLE DATA SHARING?

Organised by Computer Law and Security Review
Moderator: Sophie Stallia-Bourdillon, University of Southampton (UK)
Speakers: Étienne Feikje van der Berg, Datawallet (DE); Malte Malte Beyer-Katzenberger, European Commission (EU); Paul Comerford, Information Commissioner’s Office (UK); Alexis Wintour, Lapin, Jersey

Attempts to set up repeatable mechanisms or structures to support the accountable multi-party sharing of personal data have not yet succeeded, although different models are now emerging. The extraordinary situation of the global pandemic makes it crystal clear that there is an urgent need to accelerate the sharing of personal data among different types of stakeholders, e.g. healthcare providers, social care providers, researchers and public health authorities. However, the danger is that data subject rights will be watered down, and more generally that such data sharing will de facto enable extensive surveillance programmes and irremediably undermine fundamental rights and liberties of data subjects.

The purpose of this panel is to discuss barriers to the sharing of personal data as well as necessary safeguards, and explore a variety of emerging multi-party data sharing models across jurisdictions.

- How can we accelerate data sharing between multi parties without watering down data subject rights?
- What are the emerging multi-party data sharing models?
- How do these models compare with each other?

18:30 - TITLE TBC
Organised by EPIC

19:45 - EPIC, CNIL INRIA PRIVACY AWARD
Organised by EPIC, CNIL INRIA

CPDP2021 PANELS AT ONLINE 4

8:45 - PANEL TBC
Coming soon

10:00 - Coffee Break

10:30 - USING HEALTH DATA IN PANDEMICS: THE ISSUES AHEAD

Organised by PANELFIT Project
Moderator: Paolo Guarda, Universita di Trento (IT)
Speakers: Itigo de Miguel Beriain, University of the Basque Country (ES); Federica Lucivero, University of Oxford (UK); Claire Gayrel, EDPS (EU); Ricardo Baeza-Yates, Former CTO of NTENT (US)

In pandemic situations it is necessary to implement all the tools at our disposal to protect public health. This includes using personal data to prevent infection or to improve the diagnosis or treatment of the disease. In this panel we will discuss the ethical and legal issues involved. We will explore the legal bases that can be used for data processing, the rights of data subjects, the use of data for research, etc. We will also address a little-explored issue: the processing of medical records of deceased patients. This is a particularly complicated issue because the data of deceased people are not their personal data, according to the GDPR. Similarly, data from digital health tools offer problems of different kinds, such as the mixing of personal and non-personal data that have been insufficiently analysed.

- How can we deal with data produced by digital health devices?
- What are the legal issues involved in using AI in a pandemic situation?
- What should be the regulatory framework of health records of deceased people?
- What are the main issues involved in using health data for research purposes?

11:45 - EXPOSURE NOTIFICATION DURING THE COVID-19 PANDEMIC: RECONCILING FUNDAMENTAL RIGHTS AND PUBLIC HEALTH WITH LEGALITY ATTENTIVE DATA SCIENCE

Organised by LEADS and NIST
Moderator: Giovanni Comandé, Sant’Anna School of Advanced Studies (IT)
Speakers: René Peralta, NIST (US); Carmela Troncoso, EFPJ (CH); Michael Veale, UCL (UK); Estelle Massé, Access Now (BE); Paolo Vineys, Imperial College (UK)

- To what extent arrangements that have been built for health data in the context of the covid crisis can be repeated and generalized?
The COVID-19 global pandemic has highlighted a tension between efforts to collect sensitive personal information at scale to combat the spread of disease and potential invasions of important fundamental rights. Advancements in cryptographic techniques and other privacy enhancing technologies have allowed public health officials to move beyond manual contact tracing and consider automated contact tracing or “exposure notification” tools to help mitigate the rapid spread of illness. Yet the public continues to vigorously debate how these technologies can impact fundamental rights well beyond data protection. The panel will explore the technological, legal, and ethical dimensions of automated contact tracing and exposure notification technologies, looking for paths to reconcile tracking or data collection for public good and fundamental rights. The discussion will be an opportunity to:

1. explore the applicability of exposure notification in various use cases, and debate the merits of different cryptographic protocols and other techniques that may be used to operationalize the tool;
2. test the interplay of the fundamental right to data protection with other fundamental rights enshrined in constitutions and international charters; and
3. put in a practical context the role of technical decisions to sustain the protection of fundamental rights.

This interdisciplinary dialogue reflects the urgency to train new leadership of legality attentive data scientists and experts in data-driven technologies.

- What is exposure notification, and how does it differ from manual contact tracing?
- Do different approaches have different risks for fundamental rights and liberties?
- Use cases: Effectiveness of exposure notification for the general public versus for smaller communities or controlled environments
- Potential tradeoffs between data collection at scale and privacy harms to individuals/risk to organizations; is tracking for public health (e.g. to contain COVID-19 spreading) different from other tracking goals? Who should be setting the boundaries?
- How can technology help to create anonymous data (“personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable”) GDPR referral 26) enabling innovative technical and organisational measures to reach privacy-by-design and privacy-by-default standards? Who will be able to define and assess them? Which skills are required?

15:30 - Lunch Break

14:15 - DARK BY DESIGN: REGULATING MANIPULATION IN ONLINE ENVIRONMENTS

Organised by: SnT, University of Luxembourg
Moderator: Arianna Rossi, SnT, University of Luxembourg (LU)
Speakers: Estelle Hary, CNIL (FR); Ailo Krogh Ravna, Forbrukerradet (NO); Anne-Jel Hoelen, Authority for Consumers and Markets (NL); Cristina Teixeira Santos, Utrecht University (NL); Frederik Zuidervenne Borgesius, iHub & iCiS Institute for Computing and Information Sciences, Radboud University Nijmegen (NL)

Online services are scrupulously designed to offer the best experience to their users, accommodate their needs and direct their actions towards desirable outcomes. Yet, online services can also use manipulative design strategies to circumvent the tenets of transparency, fairness, and data protection by design.

Such strategies are known as “dark patterns”. They can restrict the number of available choices to trick users into accepting privacy-invasive features or make it overly difficult to access, transfer or erase personal data, thus hindering data subjects from exercising their rights. Dark patterns create an unequal playing field, where some companies illegitimately gather massive amounts of personal data.

This panel will discuss possible interventions, including regulatory decisions interpreting data protection principles, guidelines on best design practices, awareness-raising initiatives, and empirical studies demonstrating the influence of manipulative designs.

- How pervasive are manipulative designs in online services and what is their impact on users?
- Which tools, skills, and resources are needed to support the enforcement of rules that regulate manipulative designs?
- Which incentives might encourage businesses to prefer fair designs over dark patterns?
- How might we design interventions that enhance people’s ability to protect themselves from online manipulation?

15:30 - Privacy, Globalization and International Data Transfers: Towards a New Paradigm after Schrems II?

Organised by: CEU San Pablo University - Google Chair on Privacy, Society and Innovation
Moderator: José Luis Pilar Mañas, CEU San Pablo University (ES)
Speakers: Yann Padova, Baker McKenzie (FR); Noah Joshua Phillips, Federal Trade Commission (US); Isabelle Vereecken, EDPB (EU)

In the context of globalization and an increasingly interconnected world, an analysis of the scenario following CJEU Judgment in the Schrems II Case is essential. Identifying how companies and different actors in the field of technological innovation will operate is a real challenge. In any case, DPAs will play a key role when interpreting and applying the content of this court decision. Experts’ opinion on this matter will be essential to understand how data flows will be carried out on both sides of the Atlantic.

- What will be the real impact of this Case in the near future, in particular in relation to data transfers between the different EU countries and the USA?
- What impact will this CJEU Judgment have in our economy, taking into account the current pandemic and the economic recovery and its links with data flows and technological innovation?
- Would it be relevant at this juncture to assess the need for an in-depth analysis of what the concept of an essentially equivalent level of personal data protection entails?
- With the aim of optimizing the possibilities offered by international data flows between public and private actors, how will the different GDPR transfer tools be articulated in this new scenario?

17:15 - Schrems II: Looking Back and Looking Forward

Organised by: The Cordell Institute for Policy in Medicine & Law (Washington University in St. Louis)
Moderator: Judith Rauhofer, University of Edinburgh (UK)
Speakers: Alan Butler, EPIC (US); Ashley Gorski, ACLU (US); Neil Richards, Washington University in St. Louis (US); Andrew Serwin, DLA Piper (US)

Hear from the experts whose evidence in Schrems II was the basis for the CJEU’s blockbuster decision last July. Learn more about the trial in Dublin and what they found surprising, or not, about the Schrems II decision from the Luxembourg court. Given the evidence the CJEU conclusions were based on, how should practitioners navigate Schrems II until and unless the U.S. and EU regulators fall in line? What safeguards, rights and remedies does Schrems II really demand? Is there a path forward for a Safe Harbor 3 or even U.S. adequacy? The panelists will offer thoughtful and diverse perspectives from the private sector, academia, and civil society.

- What was the evidence that the CJEU relied on that brought us here, and how was it produced?
- What aspects of the Schrems II decision were surprising to you as a participant, or not?
- How should we navigate the fallout of Schrems II unless or until other laws are changed to comply with the decision?
- What are the ideal and most realistic paths forward for the trans-Atlantic data trade – localization, Safe Harbor 3, adequacy, or something else?
FRIDAY 29th JANUARY 2021

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

CPDP2021 PANELS AT GRANDE HALLE

8:45 – CLOSED SESSION

10:00 – Coffee Break

10:30 – CLOSED SESSION

11:45 – CLOSED SESSION

13:00 – Lunch Break

14:15 – AUTOMATED GENDER ATTRIBUTION: IT’S A BOY! IT’S A GIRL! SAID THE ALGORITHM

Organised by CPDP
Moderator Gloria Gonzalez Fuster, VUB/LSTS (BE)
Speakers Os Keyes, University of Washington (US); Sonia Katyal, University of California - Berkeley, School of Law, and Berkeley Center for Law and Technology (US); Daniel Leufer, AccessNow (BE); Karen Melchior, Member of the European Parliament (EU)

Computer says ‘male’. Computer says ‘female’. Or computer says ‘unknown’, ‘unclear but 63% chances of (X)’, or maybe just ‘error’, or ‘no’. Machines are increasingly being asked to classify individuals on the basis of their presumed gender. Daily online activities are interpreted as signs of belonging to a gender category, often without data subjects knowing about this at all, and relying on opaque grounds that can hide extremely problematic gender stereotyping. Major big tech companies base on first names crucial decisions on supposed demographics, with a direct impact on who sees which online content exactly. Bodies are being read, compared and sorted out while people just walk around in public. Automated Gender Attribution – often called Automated Gender ‘Recognition’ – is increasingly ubiquitous.

• How extensive and insidious is Automated Gender Attribution today?
• How does it affect individual rights and freedoms, including those of trans and gender non-confirming individuals?
• Can privacy and data protection laws offer meaningful protection, and how?
• What must the legislator do, notably in the context of AI regulation?

15:30 – Coffee Break

16:00 – DATA GOVERNANCE ACT: DATA PROTECTION MEETS COMPETITION, IP RIGHTS, AND INNOVATION

Organised by Uber
Moderator TBC
Speakers Simon Hania, Uber (BE); Elizabeth Renieris, Berkman Klein Center for Internet & Society (US)

The European Commission recently published the Digital Governance Act. With this Act, the Commission looks to create mechanisms to ease the sharing of public data, a system of ‘data intermediaries’ - to encourage trust in sharing personal and non-personal data - and a set of data altruism organisations’ - to facilitate the ability of individuals and companies to make data available for the common good. In this panel, we will discuss how the EC policy ambitions meet and interact with data protection, competition, and intellectual property rights as well EU fundamental rights more broadly. We will discuss what operationalizing this Act could mean in practice for cities, platform companies, and individuals.

• What tools are already available to foster data sharing in a data protection compliant manner?*
• Would data sharing affect the intellectual property rights of businesses over their activities and techniques used to process personal data?
• Is centralization of data in data trusts the answer that we are looking for?
• What consequences might have the intended European data sovereignty (i.e. data must be stored in Europe) within the context of international commerce and free trade?

17:15 – A FIRESIDE REUNION: DATA PROTECTION AT A TIME OF UNCERTAINTY

Organised by IAPP
Moderator Omer Tene, IAPP (US)
Speakers Julie Brill, Microsoft (US); Helen Dixon, DPC Ireland (IR); Bruno Gencarelli, European Commission (EU)

2020. Even just the name of the last year sends shivers down our spine. A global pandemic. Unprecedented political upheaval. Economic carnage. A fast warming planet. How do privacy and data protection fit into a dense and tumultuous policy agenda? The past year has brought to the fore issues such as access to data to mitigate a pandemic; global data transfers pursuant to Schrems II; new privacy laws in Brazil and California; and rapid developments in China and India. How do policymakers see the state of data protection at the start of 2021? What will be the issues and challenges, enforcement priorities and legislative initiatives for the coming year? Are global powers on a collision course or is a grand bargain within reach on surveillance, privacy and data protection?

• What is on the top of data protection agendas?
• What are some of the learnings from a year of privacy in a pandemic?
• What is the future of global data flows?
• What can we expect from enforcement in the EU, US and emerging data protection regimes?

18:30 – CLOSING REMARKS BY WOJCIECH WIEWIÓROWSKI
Intimate images. In particular following questions will guide the seminar:

- What role can and should social media play in preventing and removing NCII and deepnude?
- Why is online transgression of sexual integrity only so scarcely prosecuted?
- What role for civil society to tackle this phenomenon?

The humanitarian sector is, like many, exploring how to use AI to do things better, while also 'doing no harm'. Uses of AI in the humanitarian field range from detecting and evaluating the need of aid to helping in its delivery, and can emerge in complex realities in which different interests coalesce – e.g. related to security, or border control. As those benefiting from the work of humanitarian actors are frequently vulnerable populations, potentially targeted by a multitude of harmful actors, the stakes of mishandling their data, or making wrong decisions based on AI, can have consequences that go much beyond the usual risks in the digital realm. These issues demand a constant reflection on how to make sure that the potential benefits of using AI in humanitarian action are not outweighed by risks; in other terms, how to make sure that AI in humanitarian action is fully compatible with humanitarian goals.

- Which are the most pressing challenges and main opportunities of AI in humanitarian action?
- What are the implications of partnerships between humanitarian organisations and public and private actors to develop and deploy AI in the humanitarian sector?
- How to reconcile technical standards and data protection law with the humanitarian principles that humanitarian organisations are bound to respect, especially the principle of do no harm?
- How are the (best) practices developed in the humanitarian field informing data-driven Covid-19 responses?

As all aspects of human behaviour translate to the online world, so does sexual activity and interaction. With the normalisation of sexting as a regular feature for sexual development and interaction, also the abuse of such images has become a persistent digital phenomenon. Intimate images are made and distributed without consent, resulting in trauma and further abuse online as well as offline for the victims. In addition to the loss of their sexual privacy and integrity, victims are further confronted by criminal exploit of these images through sextortion and online harassment. They suffer offline consequences as loss of professional opportunities or relationships, and are hunted by phenomena of doxing to expose their identi-

- What do we define as online transgression of sexual integrity and where does the law draw the line of illegitimate behaviour?
Risks of discrimination related to the use of artificial intelligence (AI) and automated decision-making are already well-documented in several domains, including policing, hiring, loans, and benefit fraud detection. In the past year, a number of cases have indicated that the health and medical sector are not immune to the discriminatory effects of AI. Studies have shown that algorithms widely used across hospitals and health systems to guide patient care, on everything from heart surgery and kidney care, to caesarean birth and prioritizing patients following the backlog of appointments caused by coronavirus, can be racially and culturally biased, and can exacerbate existing health inequalities.

• In this panel we will discuss the risks of bias, AI-driven discrimination, and unfair differentiation in the health sector. Is there something specific to discrimination risks in the health sector?
• Are the trade-offs between the benefits and risks of AI different in this sector as opposed to other sectors?
• Is there a health sector-specific notion of fairness? If so, are sector-specific rules needed for AI in the health?
• Should legal protection against AI-driven discrimination and unfair differentiation be improved and who should attend to this: non-discrimination scholars or bioethicists?

We aim for a lively discussion panel: no presentations and no slides, but a discussion among the panelists and with the audience. The panel will be made up of experts from different disciplines and backgrounds.

18:30 – CLOSING REMARKS BY WOJCIECH WIEWIOROWSKI
in Grande Halle
Anxiety concerning the future of international data flows has reached an unprecedented peak during these last months. The Schrems II Judgment of the CJEU cast doubt about the possibility to use Standard Contractual Clauses (SCCs) for data transfers from Europe to countries that do not benefit from an adequacy decision. The post-Schrems II guidance issued by the EDPB in November 2020 accentuated this anxiety. At the same time, the CJEU, in its data retention/collection judgments of October 2020, insisted once again on the importance of adequate safeguards when data are processed for the purposes of public security. On the law enforcement side, the CLOUD Act, which has been criticized in Europe for being potentially in conflict with the GDPR, provides for the possibility to conclude agreements on LEA access to data with “qualified governments” meeting a series of safeguards. The main aim of this Panel will be to examine whether democracies could be able, through international cooperation, to respond to the challenge of setting satisfactory global standards for intelligence and law enforcement agencies access to data and to find solid and long-lasting solutions for international data transfers.

- Where do we stand with the negotiations on UK adequacy?
- Where do we stand in EU/US negotiations concerning adequacy following the invalidation of the Privacy Shield? Could non-statutory interventions respond adequately to the deficiencies in US law highlighted by the CJEU?
- Where do we stand with the EU/US negotiations for an agreement on e-evidence and CLOUD Act government access to data? What could be the effect of Schrems II on these negotiations?
- More generally, what is the future of cross-border data flows in a time of debate about “digital sovereignty”?

**16:00 – INTERNATIONAL DATA TRANSFERS: WHAT SHALL WE DO TO AVOID A SCHREMS III?**

**Organised by:** NOYB
**Moderator:** Romain Robert, NOYB (AT)
**Speakers:** Gabriela Zanfir-Fortuna, Future of Privacy (US); Max Schremms, NOYB (AT); Benoit Van Asbroeck, Bird and Bird (BE)

Two CJEU decisions and 7 years on, and despite the anxiety created by the Schrems rulings, it seems that it is still business as usual with EU-US data transfers. The guidelines of the European Data Protection Board (EDPB) and the EU Commission (COM) do not seem to be implemented in practice. Is it still possible to use US-based service providers such as Microsoft, Google, Amazon, or Apple? How can a long-term solution look like for the US? Looking beyond the US, what does the law say about transfers to the UK or to China?

- Is a risk-based approach to international transfers possible?
- What role can consent as a transfer mechanism play?
- Is it still possible to use US-based service providers without violating the GDPR?
- What does the new US administration intend to facilitate international transfers?

**17:15 – MODERN DIGITAL IDENTITY: PLUMBING, PERMISSIONING, AND PRIVACY**

**Organised by:** IoT Privacy Forum
**Moderator:** Glad Rosner, IoT Privacy Forum (ES)

The field of digital identity management (IDM) lives at the intersection of standards, commerce, engineering, policy, privacy and security. In the early 2000s, IDM was identified as a critical space in which to enact privacy values. At the same time, federated identity was evolving and growing, and e-IDs were rolling out across Europe. The appearance of social logins, like Facebook, Google and Twitter, heralded a major change in citizen identity – government agencies no longer held the monopoly on authoritative identity credentials. Now, the latest evolution in identity management is self-sovereign ID, which attempts to recreate authoritativeness through math and decentralized systems. New IDM protocols also show what’s possible in terms of actively shaping personal data flows. This panel will explore the architectures of current digital identity systems, delving into their commercial, policy, and sociological dimensions.

- What is the current state of digital identity?
- What are the relationships between self-sovereign ID, e-ID, and federated ID?
- How do commercially-derived identity and ‘official’ identity contrast?
- What can the sociology of identity papers tell us about what’s at stake in digital identity?

**18:30 – CLOSING REMARKS BY WOJCIECH WIEWIOROWSKI**

in Grande Halle
ent supervisory authorities in Chapter IV of the Directive (EU) 2016/680. However, its Article 47 of the powers of supervisory authorities is weak and vague. This panel will therefore analyse the practice of supervision of the law enforcement sector in the Digital Age.

- What do supervisory authorities need in order to have effective powers against law enforcement sector?
- Do national laws endow supervisory authorities with effective powers? How are such powers being used in everyday practice?
- Can digital investigatory measures be reconciled with the fundamental rights of privacy and data protection? What is the role of supervisory authorities in that process?
- What can we learn from statistics of inspections and corrective measures under the Directive (EU) 2016/680?

13:00 – Lunch Break


Organised by European Trade Union Institute
Moderator Alexander Fanta, Netzpolitik (AT)
Speakers Ela Jakubowska, EDRI (BE); Aids Ponce Del Castillo, ETUI (BE); Clément Nyaletsossi Voule, UN Special Rapporteur on Freedom of Assembly (INT); Birte Dedden, UNI-EUROPA (DE)

In recent years a worrying trend has become more and more visible. Surveillance practices have increased, with not only governments tracking their citizens (China’s social scoring system) but also with companies using increasingly affordable technology to monitor their workforce and collect their data. Video, tracking software, algorithmic management tools and biometric technologies, coupled with artificial intelligence and facial recognition, are bringing surveillance to potentially unprecedented levels. This raises numerous questions about privacy, workers’ and fundamental rights.

The panel will address these and other questions, present cases of workplace surveillance, as reported by European trade unions and look at the possible risks and consequences of workplace surveillance. Importantly, it will examine how fundamental rights can be used by workers and their representatives for better protection.

- Does GDPR article 88 provide sufficient protection, or does it have to be reviewed?
- What lessons can we learn from case law?
- What is the role of national Data Protection Authorities?

15:30 - Coffee Break

16:00 – TOWARD RESEARCH ACCESS FOR PLATFORM DATA

Organised by IViR
Moderator Mackenzie Nelson, AlgorithmWatch
Speakers Mathias Vermeulen, AWO (BE); Bernhard Rieder, University of Amsterdam (NL); Rebekah Tromble, George Washington University (US); Kristina Stump, European Commission (EU)

This panel explores the legal challenges of data access for public interest research into online platforms. Research access has become a key issue in platform governance debates, including not only self-regulatory initiatives such as Social Science One but also in recent ongoing reforms in the EU Digital Services Act. Platforms have commonly argued that privacy and data protection considerations pose legal and ethical barriers to research access, but these claims are now under scrutiny by academics and policymakers. Building on a recent report from the IViR, commissioned by AlgorithmWatch, this panel explores how the law in general, and data protection in particular, can help to empower the research community whilst protecting personal data.

- What access do researchers need to properly study platforms, and what legal and technical barriers do researchers face in procuring this data?
- How can platforms and governments revise their policies to facilitate independent research, and how should this be reconciled with the General Data Protection Regulation?
- What is the role of the 40 GDPR in facilitating research access through Codes of Conduct?
- What is the role of the Digital Services Act in fostering independent research access?

17:15 – DATA PORTABILITY, COMPETITION, PRIVACY, AND CYBERSECURITY

Organised by Georgia Tech
Moderator Peter Swire, Georgia Tech (US)
Speakers Régis Chatelain, CNIL (FR); Inge Graef, Tilburg University (NL); Wolfgang Kerber, Philipps Universität Marburg (DE); Nizan Packin, Zicklin School of Business (US)

Many current competition initiatives in the European Union, including the European Data Strategy, have stressed the importance of data portability for the individual, and other required transfers (often called “data sharing”) at greater than the individual scale. Portability issues have become especially timely due to: (i) their inclusion in GDPR and the California Consumer Privacy Act; (ii) intense policy focus on competition and privacy issues for the largest data-intensive platforms; and (iii) sectoral initiatives such as the Payment Services Directive II. Benefits of portability can include greater innovation and competition, and individuals’ free choice about their personal data. Risks can include privacy, cybersecurity, and anti-competitive standards.

- How should portability goals be built into important sectors such as smart cars and financial services?
- How should governance proceed on these topics, which involve data protection, consumer protection, and competition concerns?
- To what extent and when should data portability be considered primarily a fundamental rights issue, as contrasted with other regimes that seek economic efficiency and other goals?
- What should be the general lessons, during the creation of data strategies for the EU, concerning data portability?

18:30 – CLOSING REMARKS BY WOJCIECH WIEWIOROWSKI

in Grande Halle

CPDP2021 PANELS AT ONLINE 4

8:45 – CLOSED SESSION

10:00 - Coffee Break

10:30 – JUNIOR ACADEMIC SESSION I

Academic ****
Organised by CPDP
Moderator TBC
Authors Coming soon
11:45 – JUNIOR ACADEMIC SESSION II
Academic *****
Organised by CPDP
Moderator TBC
Authors Coming soon

13:00 – Lunch Break

14:15 – EDPL YOUNG SCHOLAR AWARD
Academic *****
Organised by EDPL Young Scholar Award

15:30 – Coffee Break

16:00 – SENIOR ACADEMIC SESSION III
Academic *****
Organised by CPDP
Moderator TBC
Authors Coming soon

17:15 – SENIOR ACADEMIC SESSION IV
Academic *****
Organised by CPDP
Moderator TBC
Authors Coming soon

19:45 – CLOSING REMARKS BY WOJCIECH WIEWIOROWSKI
in Grande Halle

---

**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.

**Intel**

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

**Facebook**

Founded in 2004, Facebook’s mission is to give people the power to build community and bring the world closer together. People use Facebook to stay connected with friends and family, to discover what’s going on in the world, and to share and express what matters to them.
MICROSOFT

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

APPLE INC.

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

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.

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.

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.

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.

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.
**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.

**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 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.

**STIBBE**
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.

**STIBBE**
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.

**STIBBE**
TrustArc is the leader in privacy and data protection solutions and offers an unmatched combination of innovative technology, services and TRUSTe certification solutions. TrustArc addresses all phases of privacy program management and has been delivering innovative privacy solutions for two decades to companies across all industries. The TrustArc platform leverages deep privacy expertise, integrated research and proven methodologies, which have been continuously enhanced through thousands of customer engagements. Nymity was acquired by TrustArc in 2019. Nymity provides business-friendly software solutions that minimize time to compliance with the world’s privacy laws including the CCPA, GDPR, and LGPD. Headquartered in San Francisco, and backed by a global team across the Americas, Europe, and Asia, TrustArc helps customers worldwide demonstrate compliance and accountability, minimize risk and build trust. For additional information visit www.trustarc.com and www.nymity.com.
<table>
<thead>
<tr>
<th>SPONSORS &amp; PARTNERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU</td>
</tr>
<tr>
<td>HALLES</td>
</tr>
<tr>
<td>Intel</td>
</tr>
<tr>
<td>facebook</td>
</tr>
<tr>
<td>Google</td>
</tr>
<tr>
<td>Microsoft</td>
</tr>
<tr>
<td>Apple</td>
</tr>
<tr>
<td>Mozilla</td>
</tr>
<tr>
<td>Uber</td>
</tr>
<tr>
<td>Workday</td>
</tr>
<tr>
<td>Bird &amp; Bird</td>
</tr>
<tr>
<td>BSA</td>
</tr>
<tr>
<td>epic.org</td>
</tr>
<tr>
<td>Hogan Lovells</td>
</tr>
<tr>
<td>Stibbe</td>
</tr>
<tr>
<td>Squire Patton Boggs</td>
</tr>
<tr>
<td>TrustArc</td>
</tr>
<tr>
<td>edpb</td>
</tr>
<tr>
<td>EDRi</td>
</tr>
<tr>
<td>FILIPYVER</td>
</tr>
<tr>
<td>enisa</td>
</tr>
<tr>
<td>etui</td>
</tr>
<tr>
<td>iapp</td>
</tr>
<tr>
<td>IEEE-SA</td>
</tr>
<tr>
<td>iHub</td>
</tr>
<tr>
<td>LSEC</td>
</tr>
<tr>
<td>PDP4E</td>
</tr>
<tr>
<td>PinG</td>
</tr>
<tr>
<td>IRJ</td>
</tr>
<tr>
<td>WP</td>
</tr>
<tr>
<td>CENTER FOR AI AND DIGITAL POLICY</td>
</tr>
<tr>
<td>GIPM</td>
</tr>
<tr>
<td>LUMINUS UNIVERSITY</td>
</tr>
<tr>
<td>ULB</td>
</tr>
<tr>
<td>TECHNISCHE UNIVERSITAT DARMSTADT</td>
</tr>
<tr>
<td>Digital Clearinghouse</td>
</tr>
<tr>
<td>uni. In</td>
</tr>
<tr>
<td>SOT</td>
</tr>
<tr>
<td>LSE</td>
</tr>
<tr>
<td>NIST</td>
</tr>
<tr>
<td>PRIVACY SALON</td>
</tr>
<tr>
<td>Sant’Anna</td>
</tr>
<tr>
<td>SPECTRE</td>
</tr>
<tr>
<td>School of Information Sciences</td>
</tr>
<tr>
<td>VUB</td>
</tr>
<tr>
<td>PRIVACY FIRST</td>
</tr>
<tr>
<td>BEUC</td>
</tr>
<tr>
<td>CENTER FOR DIGITAL DEMOCRACY</td>
</tr>
<tr>
<td>CDI</td>
</tr>
<tr>
<td>CENTER FOR CYBER SECURITY AND TECHNOLOGY</td>
</tr>
<tr>
<td>BRUSSELS LEGAL</td>
</tr>
<tr>
<td>MO</td>
</tr>
<tr>
<td>PRIVACY FIRST USA</td>
</tr>
<tr>
<td>PRIVACY FIRST UK</td>
</tr>
<tr>
<td>PRIVACY FIRST AUSTRALIA</td>
</tr>
<tr>
<td>visit.brussels</td>
</tr>
<tr>
<td><a href="mailto:info@cpdpconferences.org">info@cpdpconferences.org</a></td>
</tr>
<tr>
<td><a href="http://www.youtube.com/user/CPDPConferences">www.youtube.com/user/CPDPConferences</a></td>
</tr>
</tbody>
</table>