2020 brought us a magnificent English-French pop-tune by Dua Lipa and the Belgian Angèle in a unique video with only female actors and no men in sight in a buzzy London neighborhood on the kind of fever we all need.

The fever we got in 2020 was of a different nature. Skin-communication was suddenly the most needed item of the year but rare to experience. Of course there was a lot of facial privacy behind our mask, but the overall feeling amongst the privacy and data protection community was one of heightened attention to governmental and business initiatives to fight the pandemic storms.

The discussion on the Covid tracing-app was a golden one for the data protection community, since it allowed to do the things we like to do: checking on legality and appropriate safeguards. Data protection is at its strongest when it transplants a discussion in favor or against a technology by a discussion on the kind of design and (further) use of a technology. It reminded me about the body scanner discussion in the late 2000’s and how a sensible application of data protection principles and rules made a difference between overprotected badly designed body scanners and transparent and compliant scanners.

But this is conference about data protection and privacy. Not all technologies can be pimped by data protection rules and discussions about the legitimacy of high risk technologies can end with a ‘no go’ or a ‘ban’. Europe has a lot to learn from other legal regimes in this regards. Asia’s embracing of just about everything and the US’s tendency to go for banning facial technology (at least in certain areas or temporarily) are a wakeup call for our self-confidence in the solidity of data protection as a unique, self-standing framework. Angèle was probably considering our European-GDPR fascination, and not Dua Lipa, in her reply:

“Peut-être qu’avec du temps, ça partira
Et pourtant, et pourtant, et pourtant, je ne m’y vois pas
Comme un médicament, moi, je suis rien sans toi
Et je sais que j’essaie, que je perds du temps dans tes bras”

Let us meet at CPDP and continue our annual data protection and privacy discussion in this disrupted world. This year will be CPDP’s only online conference ever, so we hope. We saw it as an opportunity to enhance our faculties to bring you the best possible conference in the world, combined with a top shelf art selection that will be accessible via our digital platform. Judging the number of bios on our website (https://www.cpdpconferences.org) CPDP will host 542 speakers, 85 panels, 15 art projects exhibitions, open studios and an art bar. For the panels we created our own platform (https://2021.cpdpconferences.net). This is complemented with a social and networking platform (Gather.Town) that will please those that toyed on Second Life twenty years ago.
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

- 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)
- Diana Dimitrova (FIZ Karlsruhe – Leibniz Institute for Information Infrastructure)
- Magdalena Brewczyńska (Tilburg Institute for Law, Technology, and Society TILT)
- Imge Ozcan (Vrije Universiteit Brussel LSTS)

EXTENDED PROGRAMMING COMMITTEE

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

SCIENTIFIC COMMITTEE

- Rocco Bellanova, University of Amsterdam (NL)
- Franziska Boehm, Karlsruhe Institute of Technology, FIZ Karlsruhe – Leibniz Institute for Information Infrastructure (DE)
- Ian Brown, FGV Law School (SE)
- Paul De Hert, Vrije Universiteit Brussel LSTS (BE), Tilburg University TILT (NL)
- Willem Debeuckelaere, Ghent University (BE)
- Claudia Diaz, Katholieke Universiteit Leuven (BE)
- Michael Friedewald, Fraunhofer Institut Für System- Und Innovationsforschung ISI (DE)
- Serge Gutwirth, Vrije Universiteit Brussel LSTS (BE)
- Marit Hansen, Independent Centre For Privacy Protection ULD (DE)
- Mireille Hildebrandt, Radboud Universiteit Nijmegen (NL) & Vrije Universiteit Brussel LSTS (BE)
- Dennis Hirsch, Ohio State University Moritz College of Law (US)
- Gus Hosein, Privacy International (UK)
- Kristina Irion, Institute for Information Law (IViR), University of Amsterdam (NL)
- Els Kindt, 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, REGISTRATION & ADMINISTRATION

Privacy Salon
Rosamunde Van Brakel
Thierry Vandenbussche
Ine De Bock
Karin Neukermans
Bram Visser
www.privacysalon.org

Design © Nick Van Hee – www.nickvanhee.be
The online event will comprise two sessions and engage experts from the public health community in the EU and other international organisations to consider:

**Session 1: When will the "new normal" stop being "normal"?**
- What are the criteria that define the need for a temporary emergency measure?
- How do we determine when it is no longer necessary?

**Session 2: How can we ensure a safer and healthier digital future?**
- How can data be used to be better prepared for the next pandemic?
- How can we promote digital solidarity so that data and technology works for all people in Europe, especially the most vulnerable?

### CPDP2021 OPENING EVENT: WHO IS SOVEREIGN IN OUR DIGITAL WORLD?

**DATE** 26/1/2021 18:30 TILL 19:30  
**ORGANIZED BY** Brussels Privacy Hub, VUB-IES, UNU-CRIS and Microsoft  
**LOCATION** Online  
**REGISTER HERE** [https://brusselsprivacyhub.eu/events/cpdp2021opening.html](https://brusselsprivacyhub.eu/events/cpdp2021opening.html)

This question is paramount in relation to debates about control and cooperation in cyberspace. Digital Sovereignty provides a frame to address policy and regulatory challenges at the interface between ‘traditional’ ideas of governance and new experiments in ‘digital’ governance.

Debates around policies for recent technologies, in fields of data protection or cybersecurity, for example, emphasise the feeling that contemporary political institutions are not set up to deal with the 21st Century, neither in the way they operate, nor in the approaches they take to defining policy problems.

Please confirm your attendance to Alessandra Calvi - Alessandra.Calvi@vub.be

---

**WORKSHOP: CO-DESIGNING A VALUES-BASED FUTURE FOR DIGITAL EDUCATION**

**DATE** 25/1/2021 14:00 TILL 17:00  
**ORGANIZED BY** VUB Research Chair ‘Data Protection On The Ground’  
**LOCATION** Online  

Educational technology is predominantly steered by companies who envision the ‘future’ of education as a data-driven system in which real-time feedback, personalization, evidence-based learning, school efficiency and continuous innovation will drive and improve education. Are you thinking about how education can respond to this complex, challenging and uncertain future?

On Monday, 25 January 2021 (14:00 – 17:00 CEST), the VUB Research Chair ‘Data Protection On The Ground’ will host an online, interactive workshop under the header ‘Co-designing a values-based future for digital education’. The workshop is a side event of the Computers, Privacy and Data Protection (CPDP) conference 2021. It will be followed by a public debate on Tuesday 26 January (16:00-18:00) in a Data-Date organised by the Knowledge Centre Data & Society. During the CPDP Conference, the Chair on Data Protection On The Ground is also present on 27 January with a panel discussion on ‘Ready for a crisis: accelerated digitalization in education’.

A values-based future for teaching

At the core of this event is a workshop which draws on the Near Future Teaching Project at the University of Edinburgh, a project that was designed to engage with futures methods to craft a values-based future of teaching for the university. This workshop will help us think through the opportunities and challenges presented in the uncertainty of our current times and to articulate a ‘preferable’ future for education amidst all those probable futures available to us. We will work together to consider future scenarios and what these could mean for education.

The workshop will be accompanied by talks from distinguished speakers to help us further frame what we can expect from the next one.

Please confirm your attendance to Alessandra Calvi - Alessandra.Calvi@vub.be
<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:45</td>
<td>Closed Session</td>
<td>Online 1</td>
</tr>
<tr>
<td>10:00</td>
<td>Welcome and Introduction by Paul De Hert</td>
<td>Online 2</td>
</tr>
<tr>
<td>10:30</td>
<td>Getting AI right – can data protection help safeguard other fundamental rights?</td>
<td>Online 3</td>
</tr>
<tr>
<td>11:45</td>
<td>User Choice and Freedom through Portability and Interoperability Rights?</td>
<td>Online 4</td>
</tr>
<tr>
<td>13:00</td>
<td>Lunch</td>
<td></td>
</tr>
<tr>
<td>14:15</td>
<td>EU Digital Strategy: A holistic vision for a digital Europe?</td>
<td></td>
</tr>
<tr>
<td>15:30</td>
<td>Coffee break</td>
<td></td>
</tr>
<tr>
<td>16:00</td>
<td>EZEE: Stuck Between a Rock and a Hard Place</td>
<td></td>
</tr>
<tr>
<td>17:15</td>
<td>Enhancing Personal Data Protection through Digital Sovereignty</td>
<td></td>
</tr>
<tr>
<td>18:30</td>
<td>SIDE EVENT CPDP LATAM: NEW REGULATIONS, CROSS-BORDER DATA FLOWS, AND COVID19 IN LATIN AMERICA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Granular of holistic approach?</td>
<td></td>
</tr>
</tbody>
</table>

### Additional Sessions

**Organised by**
- CPDP
- Euroconsumers
- FRA
- EFF
- IRI (Swedish Research Institute)
- Privacy Salon
- University of Liege
- FRA
- EFF
- CPDP
- IRI (Swedish Research Institute)
- Privacy Salon
- University of Liege
- Privacy Salon
- University of Liege
- Privacy Salon
- University of Liege
- Privacy Salon
- University of Liege
<table>
<thead>
<tr>
<th>Time</th>
<th>Session A</th>
<th>Session B</th>
<th>Session C</th>
<th>Session D</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.45</td>
<td>Closed Session</td>
<td>Privacy in Automated and Connected Vehicles organised by Secredas</td>
<td>Children’s Rights in the Digital Environment: Risks, Opportunities, and Responsibilities organised by LIDERLAB</td>
<td>Closed Session</td>
</tr>
<tr>
<td>10.00</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Coffee break</td>
</tr>
<tr>
<td>10.30</td>
<td>Toward an International Accord on AI organised by Centre for AI and Digital Policy</td>
<td>Collectivize Facebook - A Pre-Trial: Transforming Facebook and other trillion-dollar companies into new transnational cooperatives under user control organised by Privacytopia</td>
<td>Standard for consent: still a dream or a soon-to-be reality? organised by Inria</td>
<td>Using health data in pandemics: the issues ahead organised by Panelfit</td>
</tr>
<tr>
<td>11.45</td>
<td>Shifting Responsibilities: The Challenges of Joint-Controllership organised by Facebook</td>
<td>Emotional AI in Smart Cities organised by Chuo University</td>
<td>Collateral Damages of Enforcement - Digital Services Act, Network Enforcement Act, and Loi Avia organised by PinG and DAV</td>
<td>Cybersecurity for Europe: Fostering rights through technology organised by Cybersec4Europe</td>
</tr>
<tr>
<td>13.00</td>
<td>Lunch</td>
<td>Lunch</td>
<td>Lunch</td>
<td>Lunch</td>
</tr>
<tr>
<td>14.15</td>
<td>Oversight and enforcement: Taking stock of design choices and trade-offs organised by Mozilla</td>
<td>Al Audits: Black Box vs. White Box perspectives organised by Haifa University</td>
<td>Algorithm-assisted decision-making in the public sector: Govern algorithms, while governing by algorithms organised by Microsoft</td>
<td>Protecting Consumers in the Data Society: It’s the Enforcement, Stupid! organised by Digital Clearing-house</td>
</tr>
<tr>
<td>15.30</td>
<td>EPIC International Privacy Award and CNIL-Inria Privacy Protection Award</td>
<td>Automated decision-making: towards effective remedies in a changing world? organised by LCII</td>
<td>Social media monitoring and movement tracking of political disidents. The end of political asylum in the EU? organised by LSTS-DIGIACT</td>
<td>Where are the missing data subjects? Democratising data protection through participation organised by SPECTRE</td>
</tr>
<tr>
<td>16.00</td>
<td>Data Sovereignty: what data is needed and how it will impact technology? organised by Intel</td>
<td>Artaccountability: Accountability, AI, and Art organised by Leiden University</td>
<td>Violent Extremism, Vulnerability and the Limits of Confidentiality organised by VUB FRC</td>
<td>Multi-party data sharing and data subjects as beneficiaries. how to accelerate accountable data sharing? organised by CSLR</td>
</tr>
<tr>
<td>17.15</td>
<td>A path to empowering user choice and boosting user trust in advertising organised by Apple</td>
<td>Introductory speech by Apple CEO Tim Cook</td>
<td>40 years of data protection and many more to come: Convention 108 and 108+ organised by Council of Europe</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>Time</td>
<td>Session 1</td>
<td>Session 2</td>
<td>Session 3</td>
<td>Session 4</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>8.45</td>
<td>Closed Session</td>
<td>Closed Session</td>
<td>Closed Session</td>
<td>Closed Session</td>
</tr>
<tr>
<td>10.00</td>
<td>Coffee break</td>
<td>Coffee break</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>
<td>Privacy of Contact Tracking Apps in Pandemic, The Role of Giant Data Collectors, and EU Sovereignty organised by TU Darmstadt</td>
<td>Fundamental rights implications of recent trends in digital forensics organised by University of Luxembourg</td>
</tr>
<tr>
<td>11.45</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>
<td>Closed Session</td>
<td>Radical insights – the fight against online radicalisation and its data protection implications organised by EDEN</td>
<td>The Effective Supervision of Law Enforcement Authorities: A Reality or A Myth? organised by MATIS</td>
</tr>
<tr>
<td>13.00</td>
<td>Lunch</td>
<td>Lunch</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>
<td>Government Access to Data after Schrems II, Brexit, and the CLOUD Act organised by Cross-Border Data Forum Panel</td>
<td>‘Smile for the camera, you are being watched’. Workplace surveillance: enforcing workers’ rights organised by European Trade Union Institute</td>
</tr>
<tr>
<td>15.30</td>
<td>Coffee break</td>
<td>Coffee break</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>
<td>International data transfers: what shall we do to avoid a Schrems III? organised by NOYB</td>
<td>Toward research access for platform data organised by IViR</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>
<td>Modern Digital Identity: Plumbing, Policy and Privacy organised by IoT Privacy Forum</td>
<td>Data Portability, Competition, Privacy, and Cybersecurity organised by Georgia Tech</td>
</tr>
<tr>
<td>18.30</td>
<td>Closing remarks by Paul De Hert (VUB) and Wojciech Wiewiorowski (EDPS)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
However, this right is not enforced and several factors hinder its success, most importantly the lack of interoperability.

Our online experience is designed by platforms having power over users and their data. A key mechanism to give users genuine choice is to give them control over their experience through interoperability and data portability measures. The upcoming Digital Services Act could tackle this issue and change the rules of the game.

The aim of the panel is to focus on portability and interoperability rights in a changing world. Presenting perspectives from academia, enforcement, policy and start-ups, the panelists will explore the gaps in legislation and give insights into what is needed for a free internet.

- What role can the rights to data portability and interoperability play in the data economy and what are the limits?
- Why is data portability so challenging to enforce?
- 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?

### 14.15 - EU DIGITAL STRATEGY: A HOLISTIC VISION FOR A DIGITAL EUROPE?

#### Speakers

- David Reichel, FRA (EU)
- Sophia Kwasny, Council of Europe (INT)
- Lilian Edwards, Newcastle University
- Pagona Tsormpatzoudi, Mastercard (BE)

The EU digital strategy sketches an ambitious approach to sculpt Europe’s digital future - covering areas and issues as diverse as the digital economy and value extraction from industrial data, to the impact of digital transformation on the environment, to the shaping of open and democratic societies. Yet, the optimal content and implementation of digital policy in Europe - of any form - is always subject to fierce contestation. A policy as ambitious as the EU Digital Strategy is no exception. In this regard, this high-level panel will seek to explore the space of the EU Digital Strategy and, in particular, will consider the following questions:

- What are the key goals of the strategy, how will they be implemented, and how will this impact exiting EU law and policy?
- To what degree does the strategy effectively balance the competing interests implied in digitisation and data processing?
- What factors will influence the successful implementation of the strategy?
- What impacts should/will the strategy have beyond Europe’s borders?

### 16:00 - E2EE: STUCK BETWEEN A ROCK AND A HARD PLACE

#### Speakers

- Scott Charney, Microsoft (UK)
- Susan Landau, Tufts University (US)
- Christine Runnegar, Internet Society (AU)

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,
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 the 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 system, 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.

What 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 could Digital Sovereignty benefit privacy and protection of personal data?

This side event will explore the latest data protection advancements, trends, and challenges in Latin America. Particular attention will be dedicated to new data protection frameworks in the region, challenges for cross border data flows, and the impact of the COVID-19 pandemic on data protection.

This debate aims at opening the path to CPDP LatAm (www.cdpd.lat), a new Latin American platform to discuss privacy, data protection and technology. CPDP LatAm encompasses the Latin American editions of the Computers, Privacy and Data Protection (CPDP) conference, the MyData conference, and Privacy Law Scholars Conference (PLSC). The 1st Latin American edition of the CPDP conference will be held in July 2021 in Rio de Janeiro, at Fundação Getulio Vargas.

This side event will focus on key issues to be further explored by CPDP LatAm 2021, which will be dedicated to Data Protection in Latin America: Democracy, Innovation and Regulation.

- Cross-Border Data Flows
- New Data Protection frameworks in LatAm
- Data protection best practices and worst practices in LatAm
- International data transfers and adequacy mechanisms

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 Sicoldone; Università Europea di Roma and InnoLawLab (IT)
Speakers: Ursula Pachi; BEUC (BE); Bart Volders, ARCAS LAW (BE); Laura Somaini, UCL (BE); Paul Breitbarth, TrustArc (NL)

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?
two years since it became applicable, the GDPR now risks becoming a “broken promise”. The one-stop-shop enforcement 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: Yasmine Boudiaf, No Tech for Tyrants (UK); Sarah Chander, European Digital Rights (BE); Nakeema Stefflauer, FrauenLoop (IE); Nani Jansen Reventlow, Digital Freedom Fund (DE); Seeta Peña Gangadharan, LSE (UK)

Historically, privacy advocates and data protection professionals envision privacy as a universal right. In practice, however, there are deep inequalities in how privacy gets enforced, who can safeguard their privacy, and what privacy means for different populations. These inequalities raise the question of whether a universalist framework reflects the lived experience of many subgroups, especially members of marginalized communities. In this provocative panel, we ask how an inclusive, collective vision of privacy looks? 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 excluded, and the exploitative nature of privacy discourse and practice in Europe.

- When and why do privacy and data protection intersect with racial justice? When do they not?
- How are privacy rights and wrongs misdistributed? And with what effect?
- Are surveillance capitalists better positioned to support racial justice efforts than digital rights advocates?
- What or who needs to change in the current configuration in the realm of privacy and data protection in order to advance racial justice?
to analyse the intersection of the deployment of new technologies, intensified surveillance and social justice with the intention of elaborating paths of action. What does the deployment of new surveillance and policing technologies look like in Europe? What is the role of the EU in these developments?

• What does the deployment of new surveillance and policing technologies look like in Europe? What is the role of the EU in these developments?
• How does the use of new technologies interconnect with the ever-growing collection of personal data and the criminalisation of certain communities?
• How does these systems pose a danger to people’s rights and freedoms, esp. of marginalised communities?
• How can we encourage civil society, activists and relevant institutions to adopt a comprehensive approach to these issues and work at their intersection?

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

Organised by PDP4E
Moderator Antonio Kung, PDP4E (FR)
Speakers Naomi Leikowitz, NIST (US); Member from PRISE team, KU Leuven (BE); Alejandra Ruiz, Tecnalia (ES); Dimitri Van Landuyt, KU Leuven (BE), Massimo Attoresi, EDPS (EU)

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 ensure the enforcement of privacy rights in such complex ecosystems. 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.

• Is privacy preserved when composing privacy friendly systems? Should we move away from a one shot, static, monodisciplinary and single perspective privacy impact assessment towards a multi-stakeholder perspective?
• How can a framework (e.g. the NIST privacy framework) help address the data protection issues raised by the multiplication of actors? Can we use it as a common framework to create an ecosystem practice for privacy rights enforcement, for instance in a data space?
• Are there specific collaboration needs between stakeholders in the ecosystem, concerning risk management, architecture and engineering practice, and contractual agreements?
• Do we need to define a roadmap on ecosystem practice, including the definition of further regulations and standards (on systems of systems, interoperability and assurance)?

8:45 - CLOSED SESSION

10:00 - Coffee Break

10:30 – TO RECORD OR NOT TO RECORD? COVID-19, BODY TEMPERATURE SCREENINGS AND THE GDPR MATERIAL SCOPE

Academic ** Policy *** Business *
Organised by CPDP
Moderator Ivan Bőröcz, VUB/LSTS (BE)
Speakers Nerea Peris Brines, European Data Protection Board (EU); Daniela Galatova, Pan-European University of Law in Bratislava (SK); Ibolya Tóth, Hungarian Authority for Data Protection and Freedom of Information (HÚ); Sandra Dobler, International Rail Transport Committee (CH); Shara Monteleone, Garante (IT)

With the onset of the Covid-19 pandemic, body temperature screening, thermal imaging and symptom tracking were some of the first measures considered in the combat against Covid-19. For a long time, there have been debates at Member State level as to whether thermal imaging and body temperature checks fall under the GDPR scope and the respective national implementing laws. Nonetheless, diverse conclusions appear to have emerged by national supervisory authorities, which reflect national differences in the application of the data protection law with respect to the use of automated and non-automated processing means, the definition of processing and the registration/archiving or not of the processed data. With body temperature screening techniques as point of departure, in this panel we will deliberate how the Covid-19 pandemic has re-heated the discussion around the GDPR material scope.

• Discuss national Covid-19 measures which may be purely analogue or combine analogue and digital components, enacted during the pandemic with emphasis on body temperature checks, and assess the importance of non-automation in EU data protection law.
• Explore national legislations and opinions issued by the national supervisory authorities in a form of a comparative analysis and in juxtaposition with the EU institutional response.
• Present and debate remarkable stances and views and explain the observed divergences and similarities.
• Study the GDPR material scope through the lenses of the pandemic.

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

Academic *** Policy **
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 Klabunde, 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 protection 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
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)

Is it practical and desirable to think about global AI governance?
What do you think other regions can learn from the initiatives and responses in your region?
Is there a need for regulatory harmonization and more harmonized research efforts in addressing the societal impacts of AI technologies.
What is the relationship between AI and DPbDD?

The development and implementation of Artificial Intelligence (AI) within all domains of business, society, and governance has accelerated in recent years. Although the current debate chiefly focuses on the economic consequences of AI, there 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 – European Union perspective; US perspective; Australian and Asia Pacific perspective; Latin America perspective. The aim is to leverage globally diverse viewpoints, and practical experience, and thereby contribute to the development of a shared understanding of 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?

15:30 – COFFEE BREAK

16:00 – PERSONAL DATA PROTECTION IN AFRICA AND IN THE MIDDLE EAST: STATE OF PLAY, CHALLENGES AND HORIZON

Academic ** Business ** Policy **
Organised by CPDP
Moderator Sophie Kwasny, Council of Europe (INT)
Speakers Marguerite Ouedraogo Bonane, DPA of Burkina Faso (BF); Omar Seghrouchni, Chair of the Moroccan DPA (MA); Sami Mohamed, Director of ADGM’s DPA (AE); Moctar Yedaly, African Union (INT); Teki Akueteth Falconer, Africa Digital Rights Hub (GH)

More and more countries in Africa and in the Middle East have adopted legal frameworks for the protection of personal information. Others are following their steps or are amending their legislations. This session will present an overview of the current state of play in the region, the opportunities to accompany many important data-driven projects and the challenges that may hinder proper enforcement of the law, especially during the current pandemic.

The panel will explore trends that may shape future legal frameworks in the region and identify pros & cons of adopting harmonized legal instrument, such as Malabo convention, Convention 108+ or a future regional GDPR-like regulation.

- State of play and trends of personal data protection legal frameworks in Africa and in the Middle East
- Most important data-driven projects in the regions that require proper personal data protection legislation.
- Challenges that may hinder proper enforcement in the region, especially during the current pandemic.
- Pros and Cons of regional legal instrument.

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

Organised by Augmented Law Institute - EDHEC Business School
Moderator Gianclaudio Malgieri, EDHEC Augmented Law Institute (FR)
Speakers Margot Kaminski, Colorado Law (US); Olivier Guillo, Smart Global (FR); Henrik Junkleuwitz, European Commission (EU); Björn Fasterling, 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 should an Algorithmic Impact Assessment should look across different Data Protection Legislations?
- Can Algorithmic DPIA and individual rights in the GDPR be connected in one tool, as a disruptive and convenient compliance model 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 Grounds
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 Seyfarth, Berinfin (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
8:45 – CLOSED SESSION

10:30 – GLOBAL YOUTH PRIVACY: AMPLIFYING YOUTH NEEDS & VOICES

Academic *** Policy ***
Organised by Privacy Salon
Moderator: Jasmine Park, FPF (US)
Speakers: Kim Noble, Comedian & co-creator of the WildLife FM theatre project (UK); Amelia Vance, Future of Privacy Forum (US); Sonia Livingstone, London School of Economics and Political Science (UK); Meghan and Mickey, young actors from the WildLife FM theatre project (UK)

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 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?

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

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

Historically, the 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 role of the OECD in the problem of data protection enforcement in the Global South?
- 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 protect 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?

13:00 – Lunch Break

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

Academic ** Business * Policy ***
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); Sizwe Snail, Information Regulator of South Africa (SA)

The panel will explore tremendous evolutions that have 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 is the enforcement of Data Protection instruments in BRICS’s countries converging (or not)?
- Are data protection legal frameworks tied, or even dependent on some level, with cybersecurity frameworks?
- Which roles and institutional functions do the BRICS’ Data Protection Authorities (DPAs) play?
- Are there specific elements of convergence 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); Andres Barreto Gonzalez, Data Protection Authority of Colombia (CO); Maryant Fernández Perez, BEUC (BE); Amanda Edmunds, Office of the Privacy Commissioner of Canada (CA)

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, and 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 it could guarantee that controllers keep control and ensure fair and lawful processing of personal data of citizens?

**17:15 - US PRIVACY LAW: THE BEGINNING OF A NEW ERA**

Academic * Business * Policy **

Organised by Future of Privacy Forum

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

**Speakers** Jared Bombom, United States Senate (US); Anupam Chander, Georgetown University (US); Stacey Schasser, Supervising Deputy Attorney General California (US); Lydia Barnes, WSGR and former director of the Bureau of Consumer Protection at the FTC (US)

Privacy is having a constitutional moment in the United States. Scholars agree, lawmakers emulate this moment to propose consequential bills and regulators show increased appetite for enforcing existing laws while preparing for stricter, new rules. The landscape is complex, to say the least. Numerous federal comprehensive privacy bills have been tabled and state initiatives push the debate forward. California, home of Silicon Valley, is leading the charge with the CCPA and its upgraded version, the CPRA. This panel will give you the pulse of how serious the US is getting about privacy law and what the world should expect next.

- What prompted the seismic shift towards privacy protection in the US?
- What are the latest privacy law initiatives at state and federal level?
- How are regulators currently enforcing existing laws and how are they preparing for what is to come?
- Will these developments manage to strengthen the Transatlantic relationship in the digital age?

**18:30 - RETHINKING ‘OPENNESS’ IN THE CONTEXT OF ARTIFICIAL INTELLIGENCE [ENDS AT 19:45]**

Organised by Centre for Intellectual Property Policy & Management (CIPPM) Bournemouth University

**Moderator** Freya van den Boom, Bournemouth University (UK)

**Speakers** Maurizio Borghi, CIPPM (UK); Brigitte Vezina, CreativeCommons (NL); Javier Ruiz Díaz, Ruiz Macpherson Ltd (UK); Michal Czerniawski, European Data Protection Board (EU)

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 access to ‘open data’ are often in a position to create proprietary or quasi-proprietary entitlements around the outcomes of algorithmically human-created works protected by copyright or neighbouring rights. Moreover, private companies who benefit from data held by public sectors open for the use and training of AI systems which is not the case for privately held data specifically.

- Can open data help advance the development and adoption of beneficial AI in society?
- How does the PSI Directive address the issue of access to data, particularly in the context of AI development?
- How can we ensure that access to data is not turned into a form of exclusive rights in reverse?

**10:00 - Coffee Break**
Advanced AI and machine- and deep learning algorithms enhance the surveillance capabilities of Law Enforcement Authorities (LEAs) and Security and Intelligence Agencies (SIAs) and are used to capitalise on new technological possibilities for modelling, processing and exploiting large data sets in unique and unexplored ways, making determinations and predictions about (innocent) people. In this way AI creates a paradigm shift in surveillance, and in state surveillance in particular, opening the doors to a new era of state surveillance, namely algorithmic state surveillance (ASS). This panel will discuss the challenges that ASS raises for existing safeguards in privacy protection and propose ways to address them in order to ensure effective privacy protection.

- What safeguards already exist against state surveillance for the protection of privacy?
- How does AI change the way how state surveillance functions?
- What challenges do algorithmic state surveillance technologies and practices raise for privacy?
- How can citizens become more aware of the use of AI in state surveillance in order to exercise their rights?

13:00 – Lunch Break

14:15 – DEMOCRATIC SURVEILLANCE? THE POSSIBILITIES AND PITFALLS OF INVOLVING DATA SUBJECTS IN DEMOCRATIC OVERSIGHT OF POLICE-USE OF SURVEILLANCE TECHNOLOGIES

Organised by: VUB Chair in Surveillance Studies
Moderator: Rosamunde van Brakel, Vrije Universiteit Brussel (BE)
Speakers: Arne Hintz, Cardiff University (UK); Quirine Eijkman, HU University of Applied Sciences Utrecht (NL); Marion Oswald, Ethics Committee West-Midlands Police (UK); Koen Gorissen, Supervisory Body for Police Information Management (BE)

The VUB Chair in Surveillance Studies panel aims to discuss the possibilities and pitfalls of citizen participation and participatory ex ante oversight mechanisms for the implementation of surveillance technologies by police. Increasingly, and also more recently triggered by the COVID pandemic, surveillance technologies for crime control and public order policing but also as management tools are implemented and experimented with. This often happens without public debate, ex ante proportionality assessments, informed DPIAs and transparency. Often, it is claimed that the data collected by the surveillance technology is anonymised or the practice is GDPR compliant, however, human rights risks for citizens and social consequences remain as no informed proportionality assessments are conducted.

In the spirit of article 35(9) of the GDPR, which states that when conducting DPIAs “where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing” - something that is not mentioned in the law enforcement directive - this panel aims to discuss the possibility of participation by data subjects and/or their representatives in ex ante oversight mechanisms. Questions we aim to answer during this panel include:

- What is the position of standing oversight bodies on involving data subjects and/or their representatives in assessing proportionality and in conducting the DPIAs?
- What should participatory ex ante oversight of police use of surveillance look like?

15:30 – Coffee Break

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

Organised by: UIUC (US)
Moderator: Chris Shenefiel, Sisco Corp (US)
Speakers: Masooda Bashir, UIUC (US); Lisa Bobbitt, CISCO Corp (US); Guy Cohen, Privitar Corp (UK); Yeong Zee Kin, InfoComm Media Development Authority (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); Mikulá Peksa, MPE (EU); Amelia Andersdotter, IEEE 802.11 (SE); Clara Neppel, IEEE (AT); Francesca Bria, Italian National Innovation Fund (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 still 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 networked 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

CPDP2021 PANELS AT GRANDE HALLE ONLINE

8:45 – CLOSED SESSION

10:00 – COFFEE BREAK

10:30 – TOWARD AN INTERNATIONAL ACCORD ON AI

Organised by Center for AI and Digital Policy (US)

Moderator Marc Rotenberg, CAIDP (US)

Speakers Tuan Nguyen, Michael Dukakis Institute (US); Malavika Jayaram, Digital Asia Hub (HK); Marit Hansen, State Data Protection Commissioner of Land Schleswig-Holstein (DE); Eva Kalli, MEP (EU)

There is growing support for an international legal framework for AI. In 2019, the OECD countries announced the AI Principles, which were then adopted by the G-20 nations. In 2020, the European Commission proposed a Transatlantic Agreement on AI. And in 2021, the Council of Europe is likely to propose an International treaty for AI, similar to the OECD Privacy Convention. All of this AI policy activity points toward the establishment of an International Accord on AI. This panel will explore the current state of affairs and the next steps.

- What are the current legal frameworks for AI?
- What are the essential elements of a global AI legal framework?
- What are the plans to establish an International accord on AI?

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, Max Planck Institute for Innovation and Competition (DE); Diletta De Cicco, Steptoe (IT/BE); Cecilia Alvarez, Facebook (ES); Karolina Możęsowicz, DG Just (EU)

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 on 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)

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 – EPIC INTERNATIONAL PRIVACY AWARD AND CNIL-INRIA PRIVACY PROTECTION AWARD


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

16:00 – DATA SOVEREIGNTY: WHAT DATA IS NEEDED AND HOW IT WILL IMPACT TECHNOLOGY?

Organised by Intel

Moderator: Riccardo Masucci, Intel (BE)

Speakers Meenakshi Lekhi, Lok Sabha (IN); Audrey Plonk, OECD (INT); Samm Sacks, New America (US); Bruno Gencarelli, DG Just, (EU)

Data sovereignty approaches are becoming more prominent worldwide. Multiple drivers are possible: 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 – A PATH TO EMPOWERING USER CHOICE AND BOOSTING USER TRUST IN ADVERTISING
Organised by Apple
Moderator: John Edwards, New Zealand Privacy Commissioner (NZ)
Speakers: Marshall Erwin, Mozilla (US), Jane Horvath, Apple (US), Lucy Purdon, Privacy International (UK), Marcel Kolaja, MEP (EU)

INTRODUCTORY SPEECH BY APPLE CEO TIM COOK
Advertising has played a crucial role in the growth of the internet. Many services that users value rely on advertising in order to provide those services. As advertising continues to evolve, how will user sentiment in relation to the creation of advertising profiles be reflected in technology? Technology solutions to provide choice and control to individuals are emerging in the market and the panel will consider how such solutions or others can be integrated into advertising practices to reflect the wishes and rights of individuals. The panel will also consider how laws such as the GDPR and many others have effectively put control in the hands of the individual. This panel is bringing together voices from Europe, Australasia and the United States to discuss and recommend actions for policymakers, regulators and all of us to help identify models of advertising which put the individual at the centre as a first step.

• How can putting control in the hands of the individual become a shared goal for all?
• Are we placing too much responsibility on individuals to make the right choices for society at large?
• What role is there for strong laws?
• What are the most compelling solutions available to tackle these problems?

18:30 – RIGHTS IN THE DIGITAL WORLD: HOW TECHNOLOGY SUPPORTS DATA PROTECTION THROUGH INNOVATIVE PRIVACY PRESERVING TECHNOLOGIES
Academic ** Business ** Policy **
Organised by Google
Moderator: Amie Stepanovich, Silicon Flatirons Center for Law, Technology and Entrepreneurship at Colorado Law (US)
Speakers: Françoise Beaufays, Google (US), Yves-Alexandre de Montjoye, Imperial College London (UK), Andrés Calvo Medina, Spanish Data Protection Authority (ES)

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.

• How can privacy preserving technology enhance digital rights and data protection?
• What are some practical advantages of privacy preserving technologies that people have benefited from already?
• In which ways can academia, civil society, and the public and private sectors collaborate further to the development and application of these technologies?
• Could public authorities accelerate the progress and adoption of this technology? In what ways?
THURSDAY 28 JAN 2021

13:00 – Lunch Break

14:15 – AI AUDITS: BLACK BOX VS. WHITE BOX PERSPECTIVES
Organised by Haifa University
Moderator Tal Zarsky, University of Haifa, Faculty of Law (IL)
Speakers Courtney Bowman, Palantir Technologies (US); Sandra Wachter, Oxford University (UK); Gianclaudio Malgieri, EDHEC Business School in Lille (FR); Jane Bambauer, University of Arizona (US)

Algorithmic decision-making has spread throughout the public and private sector, and with it, growing concerns of unfairness. These concerns have led to calls for greater transparency, especially when the processes are generated by artificial intelligence and premised on personal information. Such calls have joined actual and proposed legal requirements. A common approach to resolve transparency concerns calls for “breaking open the black box”; providing detailed information as to the algorithm’s inner workings. However, algorithm developers often strongly object to such measures, while arguing that they undermine their trade-secrets and compromise integrity by enabling gaming. These responses have led to considering auditing methods which examine the algorithm’s inputs and outputs to establish verifiable measures of accuracy and fairness. The panel will strive to establish which of these two strategies provides an optimal balance of transparency and the role that education plays in stressing the importance of being accountable in an increasingly algorithmic society.

• What solutions is industry already providing, and are they sufficient?
• Can firms meet disclosure requirements sufficiently by providing counter-factual-based explanations?
• What are the limits and benefits of auditing methods analyzing the inputs and outputs of algorithmic processes? Does a shift to this form of evaluation reflect a broader structural change from relying on procedure to examining outcomes?
• Are there lessons to be learned from the managing of the COVID-19 crisis, as to how information about AI systems should be revealed?

15:30 - Coffee Break

16:00 – AUTOMATED DECISION-MAKING: TOWARDS EFFECTIVE REMEDIES IN A CHANGING WORLD?
Organised by Liège Competition and Innovation Institute (LCII), University of Liège
Moderator Pieter Van Cleynenbreugel, LCII-University of Liège (BE)

This panel compares the emergence of emotional AI technologies in Japanese and UK/EU contexts. We will unpack the philosophical, social, ethical, cultural, legal and design questions surrounding the affect, emotion and intention in settings such as homes, workplaces and public spaces. We will reflect on how machine-readable emotions will impact fundamental rights and citizen interests, particularly in relation to information privacy, data protection and human relationships with synthetic personalities. The panel will consider some implications of data protection in the case of facial recognition and autonomous robot car in public spaces and smart cities. We will reflect on how machine-readable data will impact fundamental rights and citizen interests, particularly in relation to information privacy, data protection and human relationships with synthetic personalities. The panel will consider some implications of data protection in the case of facial recognition and autonomous robot car in public spaces and smart cities.

• How do emerging technologies change our life and what is the state of the art of emotional AI in smart cities?
• What can we learn from cross cultural perspectives on affect/emotion sensing in Japan and Europe?
• What are the proper data subjects rights and governance mechanisms for invisible sensing in smart cities?
• How do we design for an ethical life in smart cities?

17:15 – ARTACCOUNTABILITY: ACCOUNTABILITY, AI, AND ART
Organised by Leiden University
Moderator Eduard Forsch-Villaronga, Leiden University (NL)
Speakers Lucas Evers, WAAG Foundation (NL); Fiona McDermott, University of Dublin (IE); Piera Riccio, Oslo Metropolitan University, MetalAB at Harvard (NO/US); Vincent Rioux, National Superior School of Fine Arts (FR); Maranke Wieringa, Utrecht University, Data hesitate Society (NL)

This panel combines perspectives on Art, Society, & Technology. In particular, it focuses on artistic perspectives on algorithm 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 gain 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 Interplay of Art, Society and Technology
• Algorithmic Accountability and Art
• Art, Education, and Responsibility

18:30 – HOW CAN REGULATION HELP BUILD TRUSTWORTHY ARTIFICIAL INTELLIGENCE?
Academic * Business ** Policy ***
Organised by Workday
Moderator Audrey Plonk, OECD (INT)
Speakers Barbara Coagonove, Workday (US); Daniel Braun, European Commission (EU); Francesca Fellows, Squire Patton Boggs (UK); Raphael Gellert, Radboud University (NL)

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 an ecosystem of excellence. This means investing in AI capabilities and incentivising uptake by public and private sectors. And, it means setting a legislative framework that mitigates risks to fundamental rights, and ensures that technol-
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).

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.

- How should future policy and legislation frame the responsibilities of companies, authorities and regulators?
- What can companies do to build AI tools that are trustworthy-by-design?
- What role can standardisation organisations play in creating solutions?
- What are the similarities and differences between the EU approach and policies being developed in other parts of the world?
14:15 – ALGORITHM-ASSISTED DECISION-MAKING IN THE PUBLIC SECTOR: 
GOVERN ALGORITHMS, WHILE GOVERNING BY ALGORITHMS

Academic ** Business ** Policy **
Organised by Microsoft
Moderator Olivier Micol, European Commission (EU)
Speakers: Matthias Spiekamp, 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?

15:30 - 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, Juscogens (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 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.

- 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

Academia *** Business ** Policy **
Organised by Fundamental Rights Research Centre, Vrije Universiteit Brussel/ FRC, VUB
Moderator: Carlotta Rigotti, Fundamental Rights Research Centre, Vrije Universiteit Brussel (BE)
Speakers: Harald Weinbeck, Cultures Interactive (NGO) (DE); Jedrzej Niklas, School of Journalism, Media and

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

Organised by Council of Europe
Introduction by Paul De Hert, VUB (BE)
Moderator Vincent Manacourt, Politico (BE)
Speakers: Joseph A. Cannataci, Special Rapporteur on the Right to Privacy (INT); Fanny Hidski, Access Now (BE); Ulrich Kelber, Federal Commissioner for Data Protection and Freedom of Information (DE); Sophie in’t Veld, MEP (EU); Alastair Macgagant, Californians for Consumer Privacy (US)

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: utopian vision or achieved objective?
- An element of response to the contemporary transborder data flows dialectic?
- 108+: cosmetic or functional?

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?

Culture, Cardiff University (UK); Schlieman Babat, Türkische Gemeinde in Schleswig-Holstein e.V./PROvention (DE); Nora Ni Loideain, Institute of Advanced Legal Studies (IALS), University of London (UK)
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 Mantelaro, Polytechnic University of Turin (IT); Giuseppe Vaciago, R&P Legal, University of Insbruck (IT); Vanesa Gil Laredo, BBVA (ES); Marko Hölbl, University of Maribor (SI)

The recent global 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)?
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 SUBJECTS AS BENEFICIARIES: HOW TO ACCELERATE ACCOUNTABLE DATA SHARING?

Organised by Computer Law and Security Review

Moderator Sophie Stallia-Boordillon, University of Southampton (UK)

Speakers Else Feikje van der Berg, Datawallet (DE); Malte Beyer-Katzenberger, European Commission (EU); Alexis Wintour, Lapin Ltd (PT); Denise Amram, Scuola Superiore Sant’Anna (IT)

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 multiple parties?

• What are the emerging multi-party data sharing models?

• How do these models compare with each other?

• To what extent arrangements that have been built for health data in the context of the covid crisis can be repeated and generalized?

18:30 – STUDENT PRIVACY AT RISK UNDER COVID-19: ONLINE TEST PROCTORING BRINGS AI AND SURVEILLANCE INTO STUDENTS’ HOMES

Academic ** Business * Policy ***

Organised by EPIC

Moderator John Davison, EPIC (US)

Speakers Lydia X. Z. Brown, Center for Democracy & Technology (US); Meg Foukles, Open Knowledge Justice Programme (UK); Sofie van Londen, Van Londen Advocatuur (NL); Maha Bali, Center for Learning and Teaching, American University in Cairo (EG)

The use of online test proctoring has grown dramatically in the past year as educational institutions have adopted remote learning tools in response to COVID-19. This shift has forced many students to effectively trade away their privacy rights in order to meet their academic obligations. Increasingly, students must submit to invasive surveillance of their intimate spaces; compulsory collection of biometric and other sensitive personal data; and opaque AI analysis of their movements, in order to meet their academic obligations. Increasingly, students must submit to invasive surveillance of their intimate spaces; compulsory collection of biometric and other sensitive personal data; and opaque AI analysis of their movements, in order to meet their academic obligations. Increasingly, students must submit to invasive surveillance of their intimate spaces; compulsory collection of biometric and other sensitive personal data; and opaque AI analysis of their movements, in order to meet their academic obligations.

The panel will explore the technological, legal, and ethical dimensions of automated contact tracing and exposure notification during the COVID-19 pandemic.

• What should be the regulatory framework of health records of deceased people?

• What are the legal issues involved in using AI in a pandemic situation?

• How can we deal with data produced by digital health devices?

• How can we deal with data produced by digital health devices?

• What are the legal issues involved in using AI in a pandemic situation?

• How can we deal with data produced by digital health devices?

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, EPFL (CH); Michael Veale, UCL (UK); Estelle Massé, Access Now (BE); Paolo vineis, Imperial College (UK)

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. Advances 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: i) 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; ii) test the interoperability of the fundamental right to data protection with other fundamental rights enshrined in constitutions and international charters; and iii) 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.
13:00 – 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 Hoeien, Authority for Consumers and Markets (NL); Frederik Zuiderveen Borgesius, HUB & ICIS Institute for Computing and Information Sciences, Radboud University Nijmegen (NL); Geoffrey Delcroix, Ubisoft (FR)

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 – Coffee Break

16:00 – 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 Piñar Mañas, CEU San Pablo University (ES)
Speakers: Isabelle Vereecken, EDPS (EU); Noah Joshua Phillips, Federal Trade Commission (US); Alisa Vekeman, DG Just (EU); Luigi Montuori, Authority for Consumers and Markets (NL); Frederik Zuiderveen Borgesius, HUB & ICIS Institute for Computing and Information Sciences, Radboud University Nijmegen (NL); Geoffrey Delcroix, Ubisoft (FR);

In the context of globalization and an increasingly interconnected world, an analysis of the scenario following CJEU Judgments have in our economy, taking into account the current pandemic and the economic recovery and its links with data flows and technological innovation?

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 – AN EXPERT TAKE ON SCHREMS II – FROM THE EXPERTS FROM SCHREMS II
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 transatlantic data trade – localization, Safe Harbor 3, adequacy, or something else?

18:30 – WHEN REGULATORY WORLDS COLLIDE – THE INTERSECTION OF PRIVACY, COMPETITION AND CONSUMER PROTECTION
Academic ** Business ** Policy **
Organised by: GPA’s Digital Citizen and Consumer Working Group / DCCWG
Moderator: Brent R. Homan, Canadian Office of Privacy Commissioner (CA)
Speakers: Anna Colaps, EDPS (EU); Erik M. Douglas, Temple University (US); Ian Cohen, Lokker (US); Alan Campos Elias Thomaz, CT Advogados (BR)

As consumers and businesses continue to develop technology-driven commercial relationships and with personal data increasingly representing the currency of digital commerce, the overlap between the regulatory spheres of privacy, consumer protection and anti-trust has become more apparent than ever. Regulators and global networks have been living and examining this intersection of regulatory spheres. Privacy and consumer protection regulators are increasingly taking enforcement action over the same privacy related conduct. At the same time, privacy considerations have become a subject of increased discussion in the anti-trust realm, revealing complements and tensions between the two disciplines. Through this session, the cross-disciplinary panel will:

- Provide insights into the factors that have driven the intersection between privacy, competition and consumer protection and examples of intersection related-enforcement cases;
- Learn how different stakeholders (companies, regulators, policymakers) perceive and navigate the growing intersection;
- Discuss complements and tensions between the Privacy and Anti-Trust regulatory spheres;
- Discuss examples of cross-regulatory collaboration – what has worked; challenges faced; and the potential benefits.
FRIDAY 29TH JANUARY 2021

CPDP2021 PANELS AT GRANDE HALLE ONLINE

8:45 - CLOSED SESSION

10:30 - CLOSED SESSION

11:45 – 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
Moderator: Liesbet Stevens, Institute for the equality of women and men (BE)
Speakers: Cindy Southworth, Facebook (US); David Wright, UK Safer Internet Centre (UK); Catherine Van de Heyning, University of Antwerp (BE); Philipp Amann, Europol (EU)

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 such as loss of professional opportunities or relationships, and are hunted by phenomena of doxing to expose their identities. The protection of online sexual integrity is just to become even trickier with the facilitation of AI to create deepfakes without any expert knowledge required. This seminar will focus on the online transgression of sexual integrity and how to tackle this phenomenon, including the role of social media and law enforcement to prevent or tackle the distribution of these intimate images. In particular following questions will guide the seminar:

- What do we define as online transgression of sexual integrity and where does the law draw the line of illegitimate behaviour?
- 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?

13:00 - Lunch Break

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

Academic ** Business ** Policy **
Organised by: CPDP
Moderator: Gloria Gonzalez Fuster, VUB/LSTS (BE)
Speakers: Os Keyes, Washington University (US); Sonia Katyal, University of California Berkeley Center for Law & Technology (US); Daniel Leuf, 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 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. This panel will ask:

- 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: Eduardo Ustaran, Hogan Lovells (UK)
Speakers: Simon Henia, Uber (NL); Primavera De Filippi, CNRS and Berkman Klein Center for Internet & Society (FR/US); Andrea Toth, DG CNECT (EU); Oliver Micol, DG Just (EU); Gaspar Pisanu, Access Now (AR)

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 (IE); 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 PAUL DE HERT (VUB) AND WOJCIECH WIEWIOROWSKI (EPDS)
The humanitarian sector is, like many others, 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?

If we are building AI for the future we envision, AI applications must serve humanity and respect fundamental rights. The European Electronic Communications Code (ECCC) expands the notion of electronic communication services. As a result, services such as web-mail, voice over IP, instant messaging platforms and applications fall under the scope of the ePrivacy Directive as of 20 Dec 2020. To ensure that providers of online communications services can continue detecting and reporting child sexual abuse online, the European Commission has proposed an interim Regulation allowing voluntary scanning of private communication channels through “well-established” technologies. The interim Regulation attempts to provide safeguards for privacy and protection of personal data, however the instrument raises numerous concerns about its legality and proportionality.

- What technologies are currently used to scan for CSAM (image matching, text, speech analysis for child solicitation)?
- Is scanning of private communication a necessary and proportionate measure?
- What is a legal basis for the processing of personal data occurring during such scanning?
- Do the proposed safeguards ensure effective protection of the right to privacy and data protection?
Google and Apple established an unprecedented friendship and agreed on a very special scheme for contact tracing, real-

Many countries have introduced and deployed digital contact tracing apps to fight the COVID-19 pandemic. They range from heavily centralized to completely decentralized approaches, each with its own advantages and disadvantages in terms of tracing effectiveness and impact on user privacy. During the dynamic evolution of these approaches, surprisingly, Google and Apple established an unprecedented friendship and agreed on a very special scheme for contact tracing, realizing this in the form of an API called GAEN that they quickly integrated into their mobile operating systems. A multitude of nationally rolled out tracing apps are now based on the GAEN approach.

We will discuss problematic aspects and threats that the GAEN approach creates through its security and privacy weaknesses but also through the threats that it poses on the European technological sovereignty as well as the public health system:

- Digital Contact Tracing: What happened to European technological and data sovereignty?
- What happens if Google and Apple stop supporting their API or provide the app themselves?
- To what extent can sensitive information from GAEN-based app users be collected and shared?
- Despite solid alternative proposals from European scientists and experts for a digital contact tracing system, the EU has failed to establish a common system independent of giant data collectors. Why?

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 PAUL DE HERT (VUB) AND WOJCIECH WIEWIOROWSKI (EPDS)

in Grande Halle Online

CPDP2021 PANELS AT ONLINE 2

8:45 - CLOSED SESSION

10:00 - Coffee Break

10:30 - PRIVACY OF CONTACT TRACING APPS IN PANDEMIC, THE ROLE OF GIANT DATA COLLECTORS, AND EU SOVEREIGNTY

Organised by: TU Darmstadt
Moderator: Ahmad-Reza Sadeghi, TU Darmstadt (DE)
Speakers: Alexandra Dimitrienkou, University of Würzburg (DE); Patrick Breyer, MEP (EU); Claude Castelluccia, Inria (FR); Robert Riemann, EDPS (EU)

Many countries have introduced and deployed digital contact tracing apps to fight the COVID-19 pandemic. They range from heavily centralized to completely decentralized approaches, each with its own advantages and disadvantages in terms of tracing effectiveness and impact on user privacy. During the dynamic evolution of these approaches, surprisingly, Google and Apple established an unprecedented friendship and agreed on a very special scheme for contact tracing, realizing this in the form of an API called GAEN that they quickly integrated into their mobile operating systems. A multitude of nationally rolled out tracing apps are now based on the GAEN approach.

We will discuss problematic aspects and threats that the GAEN approach creates through its security and privacy weaknesses but also through the threats that it poses on the European technological sovereignty as well as the public health system:

- Digital Contact Tracing: What happened to European technological and data sovereignty?
- What happens if Google and Apple stop supporting their API or provide the app themselves?
- To what extent can sensitive information from GAEN-based app users be collected and shared?
- Despite solid alternative proposals from European scientists and experts for a digital contact tracing system, the EU has failed to establish a common system independent of giant data collectors. Why?

This panel focuses on online radicalisation in its various contexts including right wing as well as Islamist extremism. It reflects on the role of law enforcement and highlights in how far data protection plays an important role being an asset in generating trust of citizens by determining what authorities can and cannot do when processing personal data in the performance of their duties.

- Which mechanisms do extremists use in order to lure new victims into a radicalisation process?
- What are the differences between the modus operandi of right wing and Islamist extremists, if any?
- In how far do data protection rules restrict the work of law enforcement in the fight against online radicalisation and why?
- What is the role of social media and the underlying algorithms?

13:00 – Lunch Break

14:15 – GOVERNMENT ACCESS TO DATA AFTER SCHREMS II, BREXIT, AND THE CLOUD ACT

Organised by: Cross-border Data Forum
Moderator: Theodore Christakis, Université Grenoble Alpes (FR)
Speakers: Joe Jones, International Data Transfers (UK); Florence Raynal, CNIL (FR); Ralf Sauer, European Commission (EU); Peter Swire, Georgia Tech (US)

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 trans-

We will discuss problematic aspects and threats that the GAEN approach creates through its security and privacy weaknesses but also through the threats that it poses on the European technological sovereignty as well as the public health system:

- Digital Contact Tracing: What happened to European technological and data sovereignty?
- What happens if Google and Apple stop supporting their API or provide the app themselves?
- To what extent can sensitive information from GAEN-based app users be collected and shared?
- Despite solid alternative proposals from European scientists and experts for a digital contact tracing system, the EU has failed to establish a common system independent of giant data collectors. Why?

This panel focuses on online radicalisation in its various contexts including right wing as well as Islamist extremism. It reflects on the role of law enforcement and highlights in how far data protection plays an important role being an asset in generating trust of citizens by determining what authorities can and cannot do when processing personal data in the performance of their duties.

- Which mechanisms do extremists use in order to lure new victims into a radicalisation process?
- What are the differences between the modus operandi of right wing and Islamist extremists, if any?
- In how far do data protection rules restrict the work of law enforcement in the fight against online radicalisation and why?
- What is the role of social media and the underlying algorithms?

13:00 – Lunch Break

14:15 – GOVERNMENT ACCESS TO DATA AFTER SCHREMS II, BREXIT, AND THE CLOUD ACT

Organised by: Cross-border Data Forum
Moderator: Theodore Christakis, Université Grenoble Alpes (FR)
Speakers: Joe Jones, International Data Transfers (UK); Florence Raynal, CNIL (FR); Ralf Sauer, European Commission (EU); Peter Swire, Georgia Tech (US)

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 trans-

We will discuss problematic aspects and threats that the GAEN approach creates through its security and privacy weaknesses but also through the threats that it poses on the European technological sovereignty as well as the public health system:

- Digital Contact Tracing: What happened to European technological and data sovereignty?
- What happens if Google and Apple stop supporting their API or provide the app themselves?
- To what extent can sensitive information from GAEN-based app users be collected and shared?
- Despite solid alternative proposals from European scientists and experts for a digital contact tracing system, the EU has failed to establish a common system independent of giant data collectors. Why?
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 PAUL DE HERT (VUB) AND WOJCIECH WIEWIOROWSKI (EPDS)

in Grande Halle Online
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: Ella Jakubowska, EDRi (BE); Aida Ponce Del Castillo, ETUI (BE); Clément Nyaletsossi Voule, UN Special Rapporteur on Freedom of Assembly (INT); Birte Dedden, UNI-EUROPA (DE); Johannes Caspar, Hamburg Commissioner for Data Protection and Freedom of Information (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: Paddy Leerssen, IViR (NL)
Speakers: Mathias Vermeulen, AWO (BE); Bernhard Rieder, University of Amsterdam (NL); Rebekah Tromble, George Washington University (US); Krisztina 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 art. 40 GDPR in facilitating research access through Codes of Conduct?
- What is the role of the Digital Services Act in fostering independent research access
11:45 – ACADEMIC SESSION ON COVID-19 CRISIS

Academic *****
Organised by CPDP
Moderator Ronald Leenes, Tilburg University (NL)

- Wanshu Cong, European University Institute (IT): From Pandemic Control to Data-Driven Governance: the case of China’s health code
- Johannes Thumfart, VUB (BE): The Covid-crisis as catalyst for digital sovereignty: Building barriers or improving digital policies?
- Aiste Gerybaite, University of Turin (IT): Ensuring data protection rights and public safety in pandemics: lessons learnt from the Italian “Immuni” App

13:00 – Lunch Break

14:15 – EDPL YOUNG SCHOLAR AWARD

Academic *****
Organised by EDPL Young Scholar Award

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

The best 3 young authors are invited to present their research at the YSA panel. This year these will be:
- Taner Kuru, Leiden University (NL): Genetic Data: The Achilles’ Heel of the GDPR?
- Isabel Hahn, LSE (UK): Purpose Limitation in the Time of Data Power: Is There a Way Forward?
- Katherine Quezada Tavárez, KU Leuven Centre for IT & IP Law (CiTiP) (BE): Impact of the Right of Access in the Balance between Security and Fundamental Rights: Informational Power as a Tool to Watch the Watchers

The papers will be discussed with the selection jury of renowned experts Franziska Boehm, Karlsruhe Institute of Technology (DE); Alessandro Spina, European Commission (EU); Hielke Hijmans, VUB (BE) and Bart van der Sloot, Tilburg University (NL). At the end of the panel, the winner of the 5th EDPL Young Scholar Award will be revealed and receive the prize.

15:30 – Coffee Break

16:00 – SENIOR ACADEMIC SESSION

Academic *****
Organised by CPDP
Moderator Ivan Szekely, Central European University (HU)

- Andrea Bertolini, Sant’Anna School of Advanced Studies (IT) and Süreyye Elif Bilber, Sant’Anna School of Advanced Studies (IT): The Role of (Human) Dignity in AI Design Shattering the Idole of Self-Determination
- Roger Clarke, Xamax Consultancy Pty Ltd (AU): A Comprehensive Framework for Regulatory Regimes as a Basis for Effective Privacy Protection
- Mira Burri, University of Lucerne (CH): Interfacing privacy and trade

17:15 – JUNIOR ACADEMIC SESSION II

Academic *****
Organised by CPDP
Moderator Jef Ausloos, University of Amsterdam (NL)

- Thomas Tombal, University of Namur (BE): Data protection and competition law: friends or foes regarding data sharing?
- Centre Bedir, Tilburg University (NL): Contract Law in the Age of Big Data

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

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

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.

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.

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.

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.
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.

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

WORKDAY
Workday is a leading provider of enterprise cloud applications for finance and human resources, helping customers adapt and thrive in a changing world. Workday applications for financial management, human resources, planning, spend management, and analytics have been adopted by thousands of organizations around the world and across industries—from medium-sized businesses to more than 60 percent of the Fortune 50.

BIRD & BIRD
Bird & Bird is an international law firm with a focus on helping organisations being changed by technology and the digital world. With more than 1,300 lawyers and legal practitioners across a worldwide network of 29 offices, Bird & Bird specialises in delivering expertise across a full range of legal services.

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

HOGAN LOVELLS INTERNATIONAL LLP
Straight talking. Thinking around corners. Understanding and solving the problem before it becomes a problem. 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.

STEPTOE
Steptoe EU cybersecurity, data, and privacy practice focuses on existing EU and national cybersecurity, data, and privacy law. Steptoe cybersecurity, data and privacy lawyers have specific experience preparing and managing incidents in a cross-border context, where it is necessary to consider multiple cybersecurity, privacy, and other regulatory and enforcement frameworks. Steptoe provides practical and pragmatic advice to clients faced with increased accountability requirements towards users. It is helping organizations testing new responses, such as broader use of standards or certification mechanisms across the data lifecycle in a wide range of industries (regulated and not regulated). For more information, visit www.steptoe.com.

EPIC
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.

LOKKER
Lokker is a Silicon Valley-based privacy technology company that offers a robust Privacy Management Platform that enables instantaneous visibility and control over all integrated 3rd-party applications for enterprise clients. The company’s goal is to increase privacy, minimize risk, and enhance efforts to comply with international privacy regulations. Lokker’s executive team are renowned experts in privacy, data, and content delivery.

LOKKER
Lokker is a Silicon Valley-based privacy technology company that offers a robust Privacy Management Platform that enables instantaneous visibility and control over all integrated 3rd-party applications for enterprise clients. The company’s goal is to increase privacy, minimize risk, and enhance efforts to comply with international privacy regulations. Lokker’s executive team are renowned experts in privacy, data, and content delivery.

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.

STIBBE
Stibbe’s team of privacy and data protection specialists provides its clients with insight, foresight and experienced pragmatism. The team has over 20 years of experience in dealing with data protection authorities from different jurisdictions. The team is embedded in Stibbe’s TMT practice (Technology Media and Telecoms), and, as a result, the members have a thorough understanding of information technology and data communication networks. The team is involved in data governance protection projects for national and international clients, covering an a broad range sectors, such as media/entertainment, finance, communications, industry and transport, consumer goods, government and healthcare. Typical projects include privacy health checks, corporate data exchange and monitoring programs and policies.
This conference would not be possible without the industrious support of Els Vertriest, Charlotte Schaeck, Astrid Dedrie and all Medicongress staff, as well as the technical support of the wonderful people at Slash9. Also, for the mastery of our caterer KoKoen, thank you to Koen and Jordan Devolder and their team for providing such delicious food! A big thank you to Christopher Galent, Tristan Bourouze and Camille Charleux for the great partnership between CPDP and Les Halles all these years and thank you to all the staff of Les Halles for making it possible to host our technical set-up in one of the most famous and well reputed cultural centres in Brussels. To Karin Neukermans for her great work behind the scenes doing the financial administration. Many thanks also to all the volunteers and SMT students, who have done and are doing a wonderful job. In particular we want to thank Alex Dickmans, Darwin Boy Sandder, Faraniz Darvardehova, Hripsime Asatryan, Valerie Steinkogler, Yuana Kancheva. Furthermore we are thankful for the people at Josworld – Bart Vander Sanden, Agnieszka Piotrowska and Kathleen Verbesselt – who helped designing this year’s exceptional online image of CPDP.

Special thanks to all people involved in organising the side events of CPDP. Especially a big thanks to Thierry Vandenbussche who coordinatted and organised the great line up of side events including the curation of the Privacytopia events. Particularly Achim Klubunde, Aida Ponce del Castillo, Ala Kritikyce, Andy Waumam, Anemnie Vanackere, Avi Mograbii, Blancha- Ioana Marcu, Bram Visser, Clusterduck, Cynthia Burke, Daniel Leuer, Dara Hallinan, David Labi, David Murikami Wood, Ella Jakubowska, Emmanuel Van der Auwera, Faisai Hussain, Farhad Pakdel, Frederik De Wilde, Giuseppe Porcaro, Impakt Festival, Ike de Bock, Isabel Hahn, Jan Ellerman, Jordi Alba Canals, Josh Lyon, Julie Brill, Konstantina Vemou, Madelene Ashby, Marc Rotenberg, Marjin Brill, Martine Stig, Mette Birkedal Bruun, Nehal El-Hadi, Omer Tene, Paul De Hert, Peter Booth, Peter-Paul Verbeek, Piers Ricou, Rick Ferguson, Rocco Bellanova, Rosa Wewers, saava sahili singh, Sophie Kwasny, Tim Maughan, Werktank, Yasmin Boudiaf, Tactical Tech and Fanny Hidvegi. A big thank you to Gloria Gonzalez Fuster, Andrea Belu and Rocco Bellanova for organising a brilliant line-up for Privacy Camp. Thank you to the Brussels Privacy Hub for organising the pre-event.

Dara Hallinan, Ronald Leenes and Paul De Hert, the editors of the conference proceedings did a great job again. As with every year, they have produced a book of high value which leaves written proof of what CPDP is: an ambitious bet to knock down barriers among disciplines, think together, innovate and leave a mark in the privacy and data protection world. Thank you also to our brilliant team of reviewers for the CPDP2021 call for papers, all those involved in the process leading to the CPDP2021 conference book, the reviewers from the academic sessions and the second round reviewers: Aaron Martin, Alia Al-Momani, Alessandro Acquisti, Alessandro Mantelaro, Ana Fernandez Inguanzo, Andres Chomczyk Penedo, Andrew Adams, Arnold Roosendaal, Ashwinie Kumari, Bart Preneel, Bart Van der Sloot, Bettina Berendt, Bo Zhao, Chris Hoonhaghe, Claudia Diaz, Claudia Quelle, Colette Cuypers, Daniël Le Mêtre, Dennis Hirsch, Diana Dimitrova, Eduaro Celeste, Eduard Fosch Villaronga, Elvira Kostela, Eleonora Nestola, Els Kindt, Evelyn Pan, Francesco Boehm, Gabriela Zanfer-Fortuna, Georgios Bouchagiar, Gergely Biczéki, Gianclaudio Malgeri, Gianluigi Maria Ricca, Giorgio Monti, Giovanni Livraga, Gloria Gonzalez Fuster, Helen Mukri-Smith, Henrik Junklewitz, Hideyuki Matsumi, Hiroshi Miyashita, Ivan Brown, Inge Graaff, Ioulia Konstantinou, IraKlis Symeonidis, Irene Kamara, Istvan Borocz, Ivan Szekely, Joanna Kulesza, Josep Savirimuthu, Juraj Safiart, Katerina Demetzou, Kees Stuurman, Kristina Irion, Lina Jasmontaitė, Linnet Taylor, Luc Jones, Magda Brewczynska, Mara Paun, Maria Grazia Porcedda, Marit Hansen, Masa Galić, Massimo Durante, Matthieu Peeters, Maurizio Borghi, Maximilian von Graffenstein, Merel Noorman, Michael Birnhack, Michael Veale, Mistale Taylor, Nicholas Martin, Nicolò Zingales, Nora Ni Lideain, Olivier Vettermann, Orla Lynskey, Paulus Meessen, Raphael Gellert, Robin Pierce, Rosamunde van Braekel, Sara Roda, Sascha van Schendel, Shaz Jameson, Silvia De Conca, Simone Van Der Hof, Stefano Fantin, Stephanie von Maltzan, Tal Zarsky, Tineke Broer, Tsja Petrocik and Yun Shin Van Der Sype.

A special word of gratitude goes out to Nick Van Hee, our web-master and graphic designer, who has been with CPDP since the very beginning and even under great pressure always stays positive, someone with a hugely creative mind, a strenuous worker and authentic team player. Last but not least, the Programming Committee of CPDP2021 would like to thank all sponsors, conference partners, event partners, moral supporters and media partners for their generous support and everyone who has approached us with new ideas and topics for panels. Without them CPDP2021 would not have been possible!