Defining and protecting individual vulnerabilities is a relevant challenge in the data protection field. In the GDPR, the definition of “vulnerable” data subjects refers explicitly only to children, but the EDPS has often clarified that any situation of imbalance could bring to data subjects’ vulnerability: this includes cognitive issues, social and economic conditions, but also strongly asymmetric relationship (users of social media, employees vs. their employers, patients in hospitals, etc.).

The Artificial Intelligence Act is taking this challenge into account, proposing to prohibit the exploitation of some forms of vulnerability (based on age, disability or – in the Council version – even economic and social conditions), but it is very limited. However, the general definition of vulnerability proposed at Article 7 as based on a power, informational or social imbalance seems very meaningful.

The CPDP opening panel will be the opportunity to launch the “International Observatory on Vulnerable Individuals in Data protection” (IOVID), an interinstitutional project, with the aim of promoting a multi-stakeholder discussion between scholars, activists, industries and institutions on the definition and protection of vulnerable data subjects across the world.

CURATED BOOKSTAND

**Dates** 23/5/2022 8:30 till 25/5/2022 18:30  
**Organised by** De Groene Waterman - Privacy Salon  
**Location** Area 42, Rue des Palais 46, 1030 Brussels

We invited one of our favorite bookshops to select and present a surprising literature list at the conference. During the conference hours you can browse through the books, find some ‘classics’ and discover new titles.

If you like to suggest your ‘Best Of’ titles for this selection or a book launch, you can still send your proposal to books@cpdpconferences.net

TRACK TRACY INSTALLATION

**Dates** 23/5/2022 9:00 TILL 25/5/2022 18:00  
**Organised by** Privacy Salon  
**Locations** Different squares in Brussels (tbc)

Track Tracy makes a choreography with the passers-by. Two beams of light go back and forth and will follow certain people. Based on artificial intelligence, the light beams focus on a type of person who they want to put into the light. The spots that are controlled by the computer can recognize different types of people and determine which people are exposed and for how long. Track Tracy explores topics such as privacy, networking, social media and being in the spotlight. Passers-by unconsciously participate in Track Tracy’s choreography.

Before, during and after CPDP2022, the installation will travel through Brussels and confront passers-by at different squares.

Track Tracy is a creation of the artist duo Daems van Remoortere, powered by robodvision, de studio, and, district antwerpen, diederik van remoortere & domien holthof

PRIVACYTOPIA SHOWCASE

**Dates** 23/5/2022 9:00 TILL 25/5/2022 20:00  
**Organised by** Privacytopia  
**Location** Area 42, Rue des Palais 46, 1030 Brussels

Privacytopia - the art organisation behind CPDP and Privacy Salon - is taking care of artist interventions at the conference. This year, the invited Artists in Residence (AiR) are Effi & Amir. From our AiR program Marijn Bril and Emanuel Van der Auwera will present their work.

More info soon!

PECHA KUCHA NIGHT AT CPDP2022

**Date** 23/5/2022 20:00 till 22:30  
**Organised by** Architempo - Privacy Salon  
**Location** La Cave - Les Halles de Schaerbeek, Koninklijke Sinte-Mariastraat 22 a, rue Royale Sainte-Marie, 1030 Schaerbeek

Pecha Kucha is Japanese for chit-chat. The concept is a storytelling format where a presenter shows 20 slides for 20 seconds of commentary each (6 minutes and 40 seconds total). More info soon!
<table>
<thead>
<tr>
<th>Time</th>
<th>Grande Halle</th>
<th>Petit Halle</th>
<th>La Cave</th>
<th>Area 42 Grand</th>
<th>Area 42 Petit</th>
</tr>
</thead>
<tbody>
<tr>
<td>23.5</td>
<td>Registration in La Cave</td>
<td>Registration in La Cave</td>
<td>Registration in La Cave</td>
<td>Registration in La Cave</td>
<td>Registration in La Cave</td>
</tr>
<tr>
<td>7.30</td>
<td>Welcome and Introduction by Paul De Hert</td>
<td>Welcome and Introduction in Grande Halle</td>
<td>Welcome and Introduction in Grande Halle</td>
<td>Welcome and Introduction in Grande Halle</td>
<td>Welcome and Introduction in Grande Halle</td>
</tr>
<tr>
<td>8.30</td>
<td>The future of global data flows organised by IAPP (International Association of Privacy Professionals)</td>
<td>Data Protection as Corporate Social Responsibility organised by ECPC</td>
<td>Data protection regulation post-COVID: the current landscape of discussions in Europe, the US, India and Brazil organised by Data Privacy Brasil Research Association</td>
<td></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>
<td>Coffee break</td>
</tr>
<tr>
<td>10.30</td>
<td>The Future at the Intersection of Knowledge Creation, Research, and Individual Sovereignty organised by IPG KINNOSO</td>
<td>Governance and Regulation of AI from the perspective of autonomy and privacy organised by Campus Fryslân/CF</td>
<td>DPAs in the COVID-19 pandemic organised by CPDP</td>
<td></td>
<td>Genetic data: a challenge for the EU data protection framework? organised by University of the Basque Country/UPV-EHU</td>
</tr>
<tr>
<td>11.45</td>
<td>Are democratic institutions doing enough to protect democracy, freedom and privacy from the threat of unaccountable private monopoly power? organised by Open Markets Institute</td>
<td>Assessing the impact on fundamental rights in AI applications organised by Politecnico di Torino</td>
<td>Future of AI Policy organised by Center for AI and Digital Policy</td>
<td></td>
<td>A sandstorm or just a breeze? What’s the fuss about sandboxes? organised by Norwegian DPA</td>
</tr>
<tr>
<td>13.00</td>
<td>Lunch</td>
<td>Lunch</td>
<td>Lunch</td>
<td>Lunch</td>
<td>Lunch</td>
</tr>
<tr>
<td>14.15</td>
<td>The AI Act: Where are we, and where are we going? organised by CPDP</td>
<td>Title TBC organised by CPDP</td>
<td>Secondary use of personal data for (biomedical) research organised by CIIIP@KULeuven</td>
<td>Data Protection Engineering: A motorway or an intersection? organised by ENISA</td>
<td>The return of privacy? ‘Smart video surveillance’ evaluating data protection in the light of privacy and surveillance organised by VUB Chair in Surveillance Studies</td>
</tr>
<tr>
<td>15.30</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Coffee break</td>
</tr>
<tr>
<td>16.00</td>
<td>Calibrating the AI Act – is it the right framing to protect personal and fundamental right? organised by Microsoft</td>
<td>GDPR-certification schemes: General vs. specific schemes – how do effective schemes look like? organised by Alexander von Humboldt Institute for Internet and Society</td>
<td>Sharing the digital me – a contextual integrity approach for discussing governance of health and genetic data in Cyberspace organised by Uppsala University</td>
<td>Schrems II: 18 months later: much ado about nothing or a game changer? organised by EDPS</td>
<td>Encoding identities: the case of commercial DNA databases organised by University of Amsterdam</td>
</tr>
<tr>
<td>17.15</td>
<td>Regulation of global data flows: a story of the impossible? organised by EDPS</td>
<td>The AI Act and the context of employment organised by European Trade Union Institute</td>
<td>Manipulative Design Practices Online: policy solutions for the EU and the US organised by TACD</td>
<td>Digital platforms, the new privacy champions? Between myths and realities organised by Computer Law and Security Review</td>
<td>Effective transparency and control measures (including privacy icons): the example of cookie banners. Where do we stand now? organised by Berlin University of the Arts</td>
</tr>
<tr>
<td>18.30</td>
<td>Cocktail sponsored by EDPS in Le Village</td>
<td></td>
<td></td>
<td></td>
<td>Cocktail sponsored by EDPS in Le Village</td>
</tr>
</tbody>
</table>
# Computers, Privacy & Data Protection

<table>
<thead>
<tr>
<th>Time</th>
<th>Grande Halle</th>
<th>Petite Halle</th>
<th>Area 42 Grand</th>
<th>Area 42 Petit</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.30</td>
<td>Registration in La Cave</td>
<td>Registration in La Cave</td>
<td>Registration in La Cave</td>
<td>Registration in La Cave</td>
</tr>
<tr>
<td>8.45</td>
<td>Title TBC organised by DG Just</td>
<td>See you in court! - Discussing the potential and challenges of private actions for GDPR infringements organised by ALTEP DP</td>
<td></td>
<td></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>The future of privacy. How is multistakeholderism shaping privacy worldwide? organised by Apple</td>
<td>Concrete and workable solutions to the GDPR enforcement organised by NOYB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.45</td>
<td>Leveraging AI: Risks &amp; Innovation in Content Moderation organised by Meta</td>
<td>Interdisciplinary data protection enforcement in the digital economy organised by BEUC</td>
<td></td>
<td></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>Data in democracies: re-framing data use organised by The Ditchley Foundation</td>
<td>Collectively making it work: (f)laws of individual approaches to resist platform power organised by IViR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.30</td>
<td>CNIL-Inria Privacy Award, EPIC Champion of Freedom Award</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Coffee break</td>
</tr>
<tr>
<td>16.00</td>
<td>Title TBC organised by Google</td>
<td>Dark Patterns and Data-Driven Manipulation organised by Leiden University</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17.15</td>
<td>Data protection and high-tech law enforcement – the role of the Law Enforcement Directive organised by FRA</td>
<td>Mobility data for the common good? On the EU Mobility Data Space and the Data Act organised by FPF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18.30</td>
<td>Cocktail in Le Village</td>
<td></td>
<td></td>
<td>Cocktail in Le Village</td>
</tr>
<tr>
<td>7.30</td>
<td>Data Protection Friendship: the EU and Japan organised by Chuo University</td>
<td>Data protection in Asia organised by CPDP</td>
<td>GoodBrother: Privacy, Coronavirus, and Assisted Living Technologies organised by Cost Action 19121 ‘GoodBrother’</td>
<td></td>
</tr>
<tr>
<td>10.00</td>
<td>Coffee break</td>
<td>PANEL TBC</td>
<td>Responsible IoT in public space - who is actually responsible for what? organised by University Twente / Project BRIDE</td>
<td></td>
</tr>
<tr>
<td>10.30</td>
<td>The Future of the Right to Access organised by INRIA</td>
<td>Police: We can’t stand loosing you - Fortnite undercover avatars are only the beginning organised by EDEN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.45</td>
<td>Data in democracies: re-framing data use organised by The Ditchley Foundation</td>
<td>Collectively making it work: (f)laws of individual approaches to resist platform power organised by IViR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.30</td>
<td>Data Protection Certification – International Perspective and Impact organised by Mandat International</td>
<td>Data Protection in Africa and the Middle East organised by CPDP</td>
<td>Privacy design, dark patterns, and speculative data futures organised by University of Luxembourg</td>
<td></td>
</tr>
<tr>
<td>16.00</td>
<td>Title TBC organised by Mozilla</td>
<td>Data Protection in Africa and the Middle East organised by CPDP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18.30</td>
<td>Cocktail in Le Village</td>
<td>Data Protection in Africa and the Middle East organised by CPDP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Tuesday 24th May 2022**

Please note that this is a preliminary version of the programme.
<table>
<thead>
<tr>
<th>Time</th>
<th>Grande Halle</th>
<th>Area 42 Grand</th>
<th>Petite Halle</th>
<th>La Cave</th>
<th>Area 42 Petit</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.30</td>
<td>Registration in La Cave</td>
<td>Registration in La Cave</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.45</td>
<td>Title TBC organised by CDSL</td>
<td>From Shareholder Value to Social Value organised by IEEE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.00</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td></td>
</tr>
<tr>
<td>10.30</td>
<td>Practical Legal Perspectives on International Transfers organised by CPDP</td>
<td>Building Privacy as a Global Infrastructural Default - The Decentralised Approach organised by Nym Technologies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.45</td>
<td>International Transfers on the Ground organised by CPDP</td>
<td>Power over data and algorithms: can we get it back? organised by Ada Lovelace Institute</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13.00</td>
<td>Lunch</td>
<td>Lunch</td>
<td>Lunch</td>
<td>Lunch</td>
<td></td>
</tr>
<tr>
<td>14.15</td>
<td>Will the digital ever be non-binary? The future of trans (data) rights organised by CPDP</td>
<td>Is a European data strategy without trade-offs between economic efficiency and fundamental rights protection possible? organised by Open Future Foundation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.30</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td>Coffee break</td>
<td></td>
</tr>
<tr>
<td>16.00</td>
<td>Trust &amp; transparency in AI: Discussing how to unpack the “black box” organised by Uber</td>
<td>Limits of Emergency Powers: Protecting Privacy in Exceptional Circumstances organised by EPIC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17.15</td>
<td>Why privacy matters and the future of data protection law organised by Washington University</td>
<td>When Privacy and data protection rules, what and who loses out? organised by Interdisciplinary Hub for Digitalization and Society</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18.30</td>
<td>Closing Remarks by Paul De Hert and Wojciech Wiewiórowski (EDPS)</td>
<td>Closing Remarks in Grande Halle</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19.00</td>
<td>Cocktail in Le Village</td>
<td>Cocktail in Le Village</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The resolution of friction between personal sovereignty and the shared fruits of scientific and private research are a necessity as society accelerates into the digital age, where observational technology enables connected marketplace, commerce, and government. This future will be heavily reliant on the utility of technology that observes and technology that algorithmically processes data that relates to people, things, and places, both for insight (knowledge discovery) and research (academic and commercial) and then make decisions lawfully based on that knowledge. This friction is very much in play in numerous legislative and regulatory proceedings. It has been exacerbated by the acceleration of observational technology.

This session will discuss more nuanced approaches to fair governance of an observational age.

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

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

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

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

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

**Business ★ Policy ★★★★★**

Organised by EDPS

**Moderator** Wojciech Wiewiórowski, EDPS (EU)

**Speakers** Vera Jourova, European Commission for Values and Transparency (EU); Ulrich Kelber, Federal Commissioner for Data Protection and Freedom of Information (DE); Ana Brian Nougères, United Nations (UN); Audrey Plonk, OECD (FR)

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

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

### 08:45 - DATA PROTECTION AS CORPORATE SOCIAL RESPONSIBILITY

**Academia ★ Business ★ Policy ★**

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

**Moderator** Paolo Balboni, ECPC, Maastricht University (NL)

**Speakers** Sophie Nerbonné, CNIL (FR); Stefano Fratta, Facebook (IT); Sarah Bakir; Rabobank (NL); Massimo Marelli, ICRC (IT)

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

- What are the fundamental requirements of socially responsible data processing activities?
- How can data protection serve as an asset for a company to responsibly further its economic targets?
- How can companies reconstruct Data Protection into an effective CSR framework?
- What are the benefits for companies that embrace data protection as a CSR?

**CPDP2022 PANELS AT AREA 42 GRAND**

**10:00 - COFFEE BREAK**

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

**Academic ★ Business ★ Policy ★**

Organised by Campus Fryslân/CF (NL)

**Moderator** Andrej Zwitert, Campus Fryslân/CF (NL)

**Speakers** Linnet Taylor, Tilburg Law School/TLS-TILT (NL); Elizabeth Coombs, Consultant (AU); Catherine Jasseron, KU Leuven (BE); Oskar Gstrein, Campus Fryslân/CF (NL)

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

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

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

**Academic ★ Business ★ Policy ★★★**

Organised by Politecnico Di Torino (IT)

**Moderator** Anna Buchta, EDPS (BE)

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

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

- Are there different types of artificial intelligence risk assessment and, if so, what are they?
- Who should be entrusted with conducting HRIAs, when and how?
- What are the key criteria that fundamental rights impact assessments need to fulfil, in order to achieve the intended...
How far do these certification schemes meet the regulatory objectives?

What schemes have been approved by data protection authorities/EDPB so far?

What are the pros and cons of general and specific certification schemes?

What are the regulatory objectives of Articles 42 and 43 GDPR?

Can the AI Act clearly ban both mass surveillance and worker surveillance?

Can the AI Act address the specificity of AI uses in employment, including platform work?

How can HRIA be operationalised in the context of AI by providing measurable thresholds for risk management and human rights due diligence?

How can GDPR be effectively implemented in the context of employment?
Scientific research in biomedical sciences is largely based on the availability of data. Due to the limitations of anonymization techniques, these data are often personal data. Biomedical research, for example, relies on the patients’ participation and on the use and reuse of special categories of personal data, such as data concerning health and genomic data. The fight against COVID-19 caused several official bodies, amongst which the European Data Protection Board (EDPB), to emphasise that The General Data Protection Regulation (GDPR) is not intended to hinder the secondary use of (special categories of) personal data for the purpose of scientific research. However, as evidenced by several recent studies, variation in interpretation of the GDPR and national level legislation linked to its implementation have led to a fragmented approach, which brings uncertainty.

Countries have agreed on the need to prohibit social scoring, but there is still no consensus on the need to prohibit facial surveillance. What steps are necessary to achieve that goal?

How does endorsement of principles by countries compare to their practices?

What are the prospects for the EU AI Act?

Which key AI policy developments should we expect in 2022?

Deceptive design practices, or 'dark patterns', are used to make consumers take actions against their own interests, to the benefit of companies. Common privacy-invasive dark patterns include hidden default settings that maximise data collection, ambiguous language designed to confuse, and consent flows that push toward certain choices. Such practices are particularly damaging in the context of the surveillance economy, when used by the large platforms to increase their market power.

The harms caused by dark patterns are not distributed evenly and have a higher impact on people in vulnerable situations, those with low incomes, children, the elderly, or those with disabilities. Existing policies, such as the GDPR in the EU or US FTC’s section 5 regulations, are not fully equipped to deal with manipulative design practices at scale. However, legislative initiatives are taking place on both sides of the Atlantic.

What are the drivers/business objectives of 'dark patterns'?

How can dark patterns impact individuals and society generally?

What role plays the contextual integrity framework to think governance further?

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

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

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

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

The EU data protection legal framework was built around the data subject. Normally, we assume that this is a single person. This is not always the case when we consider health data in general and genetic data in particular. There are thousands of diseases that have a genetic component. This component is sometimes inheritable. This means that if we gain knowledge of a genetic component, relatives may be involved. This information is therefore very relevant for all those involved. However, the GDPR is mainly built on the individual. This perspective does not work so well with the type of issues that genetic information raises.

This panel is constituted to analyse such issues from a multidisciplinary point of view.

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

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

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

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

15:30 - COFFEE BREAK

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

- How effective has the EU been so far in applying and enforcing the CJEU Schrems II judgment?
17:15 - DIGITAL PLATFORMS, THE NEW PRIVACY CHAMPIONS? BETWEEN MYTHS AND REALITIES.

Academic Business Policy
Organised by Computer Law and Security Review
Moderator Sophie Stalla-Bourdillon, University of Southampton (UK)
Speakers
Joris Van Hoboken, Vrije Universiteit Brussel (BE); Inge Graef, Tilburg University (NL); Olivier Blazy, École Polytechnique (FR); Mehwish Ansari, Article 19 (US); Martin Bieri, CNIL (FR)

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

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

08:45 - PANEL TBC

10:00 - COFFEE BREAK

10:30 - REGULATING AI IN HEALTH RESEARCH AND INNOVATION

Academic Business Policy
Organised by Department of Innovation and Digitalisation in Law, University of Vienna (AT)
Moderator Tina Otu Anwana, University of Vienna (AT)
Speakers
Max Königsdörper, MLL Meyerlustenberger Lachenal FroSiep AG (CH); Richard Rak, University of Bologna (IT); Mariana Rissetto, University of Vienna (AT); Elisabeth Steindl, University of Vienna (AT); Mehwish Ansari, Article 19

AI systems in healthcare can help diagnose disease, prevent outbreaks, discover treatments, tailor interventions and power Internet of Health Things devices. However, the use of AI raises questions about the proper interpretation, application and interplay of EU regulations in force (GDPR, MDR/IVDR) and new legislative initiatives (AIA, European Health Data Space). The panel will debate critical data protection and AI governance challenges regarding the use of AI in health innovation and research. The speakers will discuss regulatory affairs for AI-enabled medical and ‘well-being’ devices, and the potentials and risks of new technologies in the field of mental health. In addition, the discussion will address anonymization and related risk mitigation measures concerning the use of AI in healthcare, and explore the possible implications of regulating AI in light of the foreseen European Health Data Space.

- What kind of technical and organisational measures have organisations put in place to apply the Schrems II judgment and to ensure an adequate level of protection?
- Could the adhesion of non-EU cloud operators to sovereign projects, such as Gaia-X or to the approved EU-wide cloud codes of conduct, solve the Schrems II challenge?
- How can organisations in the EU avoid non-EU government surveillance in practice and are there any lessons to be learned in this respect from the UK adequacy decisions?
- What are the regulatory concerns and challenges of using new technologies, such as big data and AI, in mental health?
- What are the implications of the AIA for the integration of AI systems with Internet of Health Things devices?
- What are the legal challenges and risks concerning the anonymisation of health data and how to mitigate the risks associated with re-identification?
- Is the interplay between the AIA and the European Health Data Space initiative enough to establish a clear set of rules applicable to AI in health research?

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

Organised by The Norwegian Data Protection Authority (Datatilsynet) (NO)
Moderator Bojana Beatty, Centre for Information Policy Leadership (CIPL) (UK/RS)
Speakers
Kari Laumann, Norwegian Data Protection Authority (NO); Chris Taylor, ICO (UK); Erlend Andreas Gjære, Secure Practice (NO)

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

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

13:00 - LUNCH

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

Organised by VUB Chair in Surveillance Studies
Moderator Rosamunde van Brakel, University of Tilburg/VUB (NL/BE)
Speakers
Ola Svenonius, Swedish Defense College (SE)
Sophie Stalla-Bourdillon, University of Southampton (UK)

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

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

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

15:30 - COFFEE BREAK
16:00 – ENCODING IDENTITIES: THE CASE OF COMMERCIAL DNA DATABASES

Academic Business Policy
Organised by University of Amsterdam (NL)
Moderator Alexandra Gjionopoulos, Institute for Information Law/IViR (NL)
Speakers Amade M’Charaf, University of Amsterdam/UvA (NL); Rossana Ducato, University of Aberdeen (UK); Taner Kuru, University of Tilburg (NL); Ella Jakubowska, EDRi (BE)

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

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

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

Academic Business Policy
Organised by Einstein Center Digital Future / Berlin University of the Arts (DE)
Moderator Birgit Sippel, Member of the EU Parliament (EU)
Speakers Estelle Hary, CNIL (FR); Max von Grafenstein, Einstein Center Digital Future (Berlin University of the Arts) (DE); Jana Krahforst, Usercentrix (DE); Michael Kleber, Google (US)

Cookie consents with manipulative information and decision architectures are ubiquitous, at least perceived to be. The problem of such so-called dark patterns has long been recognised by regulators, studied by scientists and now also fought by data protection activists. But what are positive examples of particularly successful transparency and control measures? On what lemm of such so-called dark patterns has long been recognised by regulators, studied by scientists and now also fought by data protection activists. More and more, multistakeholderism is shaping global governance of privacy and whether privacy can and should be achieved through multistakeholderism and the limits thereof.

- What are the most recent/prominent examples of good and bad transparency and control measures? On what methodological basis can these be developed, and their effectiveness tested? And what is the current state of research and development of privacy icons that are considered part of the solution? The panel will provide an overview of examples from (law enforcement) practice and the current state of research as well as possible development paths.
- What role do PIMS, CMP and browsers play in this context?
- What is the regulator’s point of view on this?
A panel discussion that reframes the central role of data to society and examines duty of care in an era where we need to enable responsible data use globally. For societies to flourish in the 21st century, government, civil society, and industry will need to invest in the appropriate use, maintenance and regulation of data while remaining committed to maximizing the societal benefit and protecting fundamental rights. The panel will examine current and future norms around the use of data globally and how policy, technical innovation and operational controls can protect the trusted free flow of data in health care, trade and government access while protecting privacy and human rights.

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

16:00 – TITLE TBC

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

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

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

- What are the respective roles of the EU Supervisory Authorities, EU institutions, and civil society organisations?
- Why do they occur?
- What are the persisting issues in the area of the GDPR enforcement?
- What solutions are there?
- What are the respective roles of the EU Supervisory Authorities, EU institutions, and civil society organisations?
have actually ‘broken’ but one thing is clear: the lines that separated various areas of law (e.g., competition, consumer protection, data protection) have been broken, or at least blurred. This creates many challenges. How can we effectively address practices which may infringe several legal instruments at the same time, in several jurisdictions, under the watch of several authorities? Bad actors seek to exploit the cracks and gaps in our system and often get away with little consequences for their actions. Whereas the gravity of those actions might sometimes seem limited when looking through a single lens, the picture quickly changes when we broaden our perspective. It is time for enforcers to move fast and break things too.

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

13:00 - LUNCH

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

Organised by IIVR (NL)
Moderator Diviž Joshi, University College London (UK)
Speakers
Anton Eikker, Ekker Advocatueur (NL); Jill Toh, University of Amsterdam, IIVR (NL); Vanessa Barth, IG Metall, FairTube project (DE); Eike Gräf, European Commission (BE)

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

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

15:30 - COFFEE BREAK

16:00 - DARK PATTERNS AND DATA-DRIVEN MANIPULATION

Organised by Leiden University (NL)
Moderator Mark R. Leiser, Leiden University (NL)
Speakers
Mireille Caruana, University of Malta (MT); Catalina Goanta, Maastricht University (NL); Egelyn Braun, European Commission (EU); Agustin Reyna, BEUC (EU)

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

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

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

Organised by Future of Privacy Forum/FPP (US)
Moderator Kelsey Finch, Future of Privacy Forum (FPP) (US)
Speakers
Laura Cerrato, Centre d’Informatique pour la Région de Bruxelles (BE); Arjan Kapeitijn, Autoriteit Persoonsgegevens (NL); Anna Ludin, European Commission DG CNECT (BE)

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

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

CPDP2022 PANELS AT PETITE HALLE

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

Organised by Amsterdam Law & Technology Institute (ALTl); VU Amsterdam (NL)
Moderator Sarah Eskens, Amsterdam Law & Technology Institute, VU Amsterdam (NL)
Speakers
David Martin Ruiz, BEUC (BE); Valentina Golunova, Maastricht University (NL); Andrea Bladarti, Privacy Network Italia (IT); Silvia De Conca, Amsterdam Law & Technology Institute, VU Amsterdam (NL)

Social media continuously moderate content on their platforms. In doing so, they need to balance the freedom of expression rights of those who upload content with the interests of other individuals and groups to remove harmful content. Platforms like Facebook and Instagram currently mix automated and human decisions. Over- and under-inclusive interventions remain, however, a daily occurrence. legitimate content is automatically taken down, harmful content sometimes remains online notwithstanding the reports of users. The GDPR provides a right not to be subject to automated decision-making but it is an open question if this right can provide redress with regard to content moderation. The new Digital Service Act introduces the right of redress for users. But what does it entail, and are there alternative solutions to explore? What are the limits of individual access to justice within privately owned online platforms?
• What is the role and what are the limitations of the redress tools against automated content moderation offered by the GDPR?
• What is the role and what are the limitations of the new right of redress introduced by the Digital Services Act against automated content moderation?
• Are there any alternatives to automated decisions implementing the T&S of a social media platform?
• Is there an "access to justice" right in the context of privately owned social media? What are its main elements?

10:00 - COFFEE BREAK

10:30 - THE FUTURE OF THE RIGHT TO ACCESS

Organised by INRIA (FR)
Moderator Cedric Lauradoux, INRIA (FR)
Speakers Cristina Santos, Utrecht University, (NL); René Mahieu, Vrije Universiteit Brussel, (BE); Sjoera Nas, Privacy Company (NL); Gene Y Tsudik, University of California, Irvine (US)

The right to access is fundamental in the GDPR. It is a great transparency tool. Lately, many studies have shown how to abuse the right to access to steal data.
1. Researchers demonstrated that it is possible to abuse the right to access to steal data from others,
2. Studies have shown that data subject access requests are often denied by data controllers.
   Why is it difficult to implement the right of access? During this panel, we will do a diagnosis of all the symptoms of the failure of the right to access. We will also try to find solutions to fix the right to access to avoid abuses and systematic denial of access and try to discuss how to fix it at the end of this panel.
   • Why is the right to access so important?
   • What threatens the right to access?
   • Right to access: transparency tool or privacy threat?
   • How to fix the right to access?

11:45 – POLICE: WE CAN’T STAND LOSING YOU – FORTNITE UNDERCOVER AVA-
TARS ARE ONLY THE BEGINNING

Organised by EDEN
Moderator Daniel Drewer, Europol (EU); Jan Ellermann, Europol (EU)
Speakers Rik Ferguson, Trend Micro (POL); Véronique Bechu, Central Unit for Minor Victims (FR); Isabelle Debré, Association L’Enfant Bleu (FR); Fabrice Plazolles, Havas Sports & Entertainment (FR)

What do a blue-winged angel, an online game and a series featuring a cyberattack against a medical company have in common? They all manifest that the future is here.
The panel focuses on the future of cyberspace and envisions how our lives and societies will be in the not-so-distant digital times to come. Véronique Bechu, Isabelle Debré and Fabrice Plazolles talk about how law enforcement, an NGO and a private company joined forces to make Fortnite a safer (cyber)space where children reported sexual abuse and other forms of serious crime, while Rik Ferguson takes us on a journey through his 2030 world.
   • How will the cyberspace and our societies look like by 2030?
   • How can online games help law enforcement protect minors from sexual abuse and other forms of crime?
   • How can law enforcement agencies, civil society and private industries collaborate to protect vulnerable groups and what are the challenges?
   • Is the cyberspace the future of police operations?

13:00 - LUNCH

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

Academia ♬ Business ♬ Policy ♬ Organised by Microsoft (US)
Moderator Ivana Bartolletti, Wipro (UK)
Speakers Michael A. Madalo, Microsoft Research (US); S.N.R. (Stefan) Builjsman, TU Delft (NL)

Research and best practices in addressing risks in AI systems have significantly progressed over the last years. This panel looks at the most challenging problems and advances in research to support fairness, accountability, transparency and equity in AI. The panel will also examine whether the AI Act’s requirements for trustworthiness will be flexible enough to address these objectives, nuanced enough to tackle the diversity of AI systems and their specific risks as well as the pace of innovation.
• Are the requirements able to tackle the socio-technical challenges of AI systems?
• What are the criteria against which the AI Act requirements will be measured?
• Are outcome-based goals an alternative?
• How can AI deployers be supported in their fairness work in practice?
• How can stakeholders impacted by AI participate in designing fairer and more responsible AI?

15:30 - COFFEE BREAK

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

Organised by Mandat International
Moderator Luca Bolognini, Italian Institute for Privacy (IIP) (IT)
Speakers Peter Kimpian, Council of Europe (EU); Catherine Lenman (CH); Fabrice Naftalski, EY Avocats (FR); Sébastien Ziegler, Mandat International European Centre for Certification and Privacy (LU); Chiara Romano, Italian Data Protection Authority (IT)

The GDPR makes over 70 references to data processing certification in line with its art. 42, including for cross-border data transfers (Art. 46). Similar certification mechanism is embedded in other data protection regulations. This session will provide an overview of the latest developments in data protection certification in Europe and internationally. The session will start by introducing the recent evolution of data protection certification. The Swiss Supervisory Authority (FDPIC) will present the experience and perspective of data protection certification in Switzerland based on many years of experience. The Council of Europe (CoE) will provide a complementary perspective on data protection certification at the international level. The European Centre for Certification and Privacy (ECCP) will present and discuss some innovative models in certifying the compliance of data processing under the GDPR and other regulations. The session will conclude by a panel discussion on expectations, challenges and opportunities with regards to international and mutual recognition of such certification.
• What are the lessons learned and opportunities with data protection certification?
• What is the potential for international recognition of data protection certification?
• What are the differences between universal, specific, and hybrid certification mechanisms? What are their benefits and disadvantages?
• What challenges organisations face following the adoption of the GDPR?
• What are the current state-of-the-art certification solutions for certifying and demonstrating GDPR compliance?

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

Academia ♬ Policy ♬ Organised by SPECTRE project (BE)
Moderator Jonas Breuer, SPECTRE/Vrije Universiteit Brussel (BE)
Speakers Yigit Aydin, European Sex Workers Rights Alliance (EU); James Farrar, Worker Info Exchange (UK); Stefania Milan, University of Amsterdam (NL); Paola Pierri, Democratic Society (EU)
Vulnerable individuals and communities are impacted by a lack of digital literacy and e-inclusion in today’s digitalised societies, which idealise the “tech-savvy, independent, and uber-modern, able to produce digital data and analyze it to hold city government accountable” as Burns and Andručik (2020) argue. This panel revisits vulnerability, zooming in on the impacts of digital technologies. It discusses how new forms of vulnerability are created, or existing ones exacerbated in societies informed through technologically mediated networks and ICT. Data subject rights may be promising tools as they aim to empower individuals and counter power asymmetries. The panel therefore looks into whether regulatory frameworks (data protection, administrative law) are mature and apt enough to tackle the challenge of protecting the rights and interests of those who find themselves increasingly marginalized while others reap the benefits of digitalisation.

In this regard, the panel aims to ask the following questions:

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

07:30 - DATA PROTECTION FRIENDSHIP: THE EU AND JAPAN

Organised by Chuo university
Moderator Hiroshi Miyashita, Chuo University (JP)
Speakers Laura Drechsler, Vrije Universiteit Brussel (BE); Kazue Sako, Waseda University (JP)

This panel will examine the recent data protection law reforms in Japan and consider the convergence between Japan and the EU. The 2019 adequacy decision for Japan was a success story for constructing the privacy bridges between the EU and Japan. This panel will explore the main regional initiatives on AI, their overlap with data protection, their intersection with human rights law, and the specific regulatory and technological approaches that are emerging and being proposed.

The importance of evidence-based policies is globally acknowledged and such evidence increasingly rely on the use of large (personal) data pool for policy planning. Public and private sector actors alike increasingly depend on personal data processing to provide their services. For Latin America, the innovative use of personal data for policy planning plays a fundamental role to reduce inequalities. However, some core challenges persist, including how to implement innovative, secure, and legally interoperable data governance systems. This CPDP Latin side event will explore some flagship initiatives and policies on data governance in Latin America.

08:45 - DATA PROTECTION IN ASIA

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

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

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

10:45 – GOOBROTHER: PRIVACY, CORONAVIRUS, AND ASSISTED LIVING TECHNOLOGIES

Organised by Cost Action 19121 ‘GoodBrother’ (EU)
Moderator: Liane Colonna, CA 19121 GoodBrother Member, Stockholm University (SE)
Speakers: Carina Dantas, European Connected Health Alliance (PT); Birgit Morlion, European Commission (BE); Eduard Fosch-Villaronga, Leiden University (NL)

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

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

11:45 – BIG BROTHER OUT TO LUNCH

Organised by PROTEIN project (EU)
Moderator: Eugenio Mantovani, Vrije Universiteit Brussel (BE)
Speakers TBC

13:00 – LUNCH

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

Organised by SN,T, University of Luxembourg (LU)
Moderator: Cristiana Santos, University of Utrecht (NL)
Speakers: Regis Chatellier, CNIL (FR); Georg Philip Krog, Signatu (NO/CH); Stefano Leucci, EDPS (EU); Dusan Pavlovic, Better Collective (SE/DS); Arianna Rossi, SN,T, University of Luxembourg (LU)

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

On the other side, the harm caused by malicious designs is increasingly being exposed and a growing number of transparency-enhancing technologies is being created to support the rights of data subjects. But we can only devise and implement overarching data protection by design if we become able of anticipating trends, explore the future implications of technology and guide its development towards desirable outcomes. In the end, which bright-er worlds do we intend to design to ensure fair, transparent, human-centred use of personal data?

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

15:30 – COFFEE BREAK

16:00 – EDPL YOUNG SCHOLAR AWARD

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

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

08:45 - TITLE TBC
Organised by CDSL

10:00 - COFFEE BREAK

10:30 - PRACTICAL PERSPECTIVES ON INTERNATIONAL TRANSFERS
Business ★★★★★ Policy ★★★
Organised by CPDP
Moderator Laura Linkomies, Privacy Laws and Business (UK)
Speakers Diletta De Cicco, Steptoe (BE); Ruth Boardman, Bird & Bird (UK); Laura Brodahl, Wilson Sonsini Goodrich & Rosati (BE)

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

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

11:45 - INTERNATIONAL TRANSFERS ON THE GROUND
Business ★★★ Policy ★★★
Organised by CPDP
Moderator TBC
Speakers Eduardo Ustaran, Hogan Lovells (UK); Rosa Barcelo, Squire Patton Boggs (BE); Alan Butler, EPIC (US); Thomas Boué BSA | The Software Alliance (BE)

Following the previous panel, this panel continues the theme of the practical issues surrounding international transfers under the GDPR. This panel takes a broader perspective and considers the real-world impact of uncertainties in the law surrounding international transfers, and efforts to resolve these uncertainties. Naturally, such uncertainties, and related policy efforts have their own logic which can produce winners and losers. With this in mind, this panel brings together speakers from different sectors and with different perspectives. Panelists will consider, amongst others, the following questions:

- What are the different types of impacts - for example on companies and individuals - from uncertainties around the law on international transfers?
- What changes have recent developments in law - for example in Schrems II - produced on the ground?
- In light of the current situation, what needs to be done moving forward?
In a world that increasingly recognises that gender cannot be understood as binary and immutable, technology and law appear to be still too often trapped in male/female classifications, leaving aside the rights, needs and concerns of those who are un- or mis-represented by such classifying canvas, and possibly harmed by it. And in a Europe lacking a consistent approach towards the recognition of gender identities, the debate on how to appropriately protect gender identities online is far from being solved. This panel will discuss privacy and data protection rights of non-binary and trans individuals, but also deeply intertwined issues around data collection and illegal and technical gender categorisation. Aiming at throwing light on how to best protect the digital rights of all, which necessarily requires taking seriously the digital rights of LGBTQ+ individuals, it will ask:

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

- Why do privacy and data protection matter? What values do they serve?
- What is the relationship between privacy and data protection rules and identity formation, political freedom, and consumer protection?
- How should our understandings of privacy and data protection change as we confront new problems like public health emergencies, artificial intelligence, and pervasive data collection and computing?
- Is a shared understanding of what privacy is and why it matters possible across the different legal systems on both sides of the Atlantic?
Today’s data infrastructures, operated and controlled by dominant tech platforms, block the way for more sustainable, pri-
tional separation of dominant platforms via interoperability measures and introducing non-commercial data intermediaries.

The panel will acknowledge risks and practical difficulties that come with transformations such as decentralisation or func-

In reaction to centralisation and data exploitation, recent years have seen a wave of decentralised technologies. New pro-
tocols, blockchains, DLTs and DAOs aim to challenge surveillance capitalism by proposing new models for the internet. This

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

Today’s data infrastructures, operated and controlled by dominant tech platforms, block the way for more sustainable, pri-
vacy-protective and user-centric business models that are accountable towards individual users and mindful of the social

The panel will discuss what regulatory, technological and institutional transformations are needed in order to reclaim the power over data and algorithms from dominant platforms to serve individual and societal goals. Invited experts will discuss the most promising avenues, which include counter-power measures that decentral tech, new types of infrastructure and new institutions that could emerge.

The panel will acknowledge risks and practical difficulties that come with transformations such as decentralisation or func-
tional separation of dominant platforms via interoperability measures and introducing non-commercial data intermediaries (such as “BBC for data”). These insights will be based on preliminary findings made by the Rethinking Data working group set up by the Ada Lovelace Institute.

• How are measures proposed in draft DMA/DSA/DGA regulations addressing the lack of dominant platforms’ accounta-
bility when it comes to their power over data and algorithms?
• Assuming that open, interoperable ecosystems replace closed ecosystems operated and controlled by dominant plat-
forms, what data protection and data security safeguards need to be in place in order to ensure accountability of new
instutions (e.g. data trusts or public interest corporations)?
• Under which conditions, including strict data protection and data security requirements, new competitors should have
access to open ecosystems, including access to aggregate personal data and ML models (so far controlled by dominant platforms)?
• What might help open the ‘gates’ for new types of data intermediaries and their use of data for social benefit, beyond
what has already been proposed in the DMA/DSA/DGA?

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

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

Today’s data infrastructures, operated and controlled by dominant tech platforms, block the way for more sustainable, pri-
vacy-protective and user-centric business models that are accountable towards individual users and mindful of the social

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

16:00 – LIMITS OF EMERGENCY POWERS: PROTECTING PRIVACY IN EXCEPTIONAL CIRCUMSTANCES
When it comes to digital harms, privacy and data protection concerns have come to dominate public debate and regulation. While useful early on in the stride against the new power asymmetries of the digital era, the focus on privacy and data protection is currently engendering detrimental effects. Amongst others, the hegemony of the value of privacy may crowd out other values that are no less important or at risk in digital society – such as solidarity, democratic control and justice – or narrowly redefine them as privacy concerns. The focus on data protection may also be counterproductive at a time when Big Tech is developing privacy-friendly ways to expand into new sectors of society. Moreover, governments may increasingly use privacy to evade discussion and critique. The panel will address the effects of the rise to dominance of privacy and data protection concerns:

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

**10:30 - MEASURING FUNDAMENTAL RIGHTS COMPLIANCE THROUGH CRIMINAL JUSTICE STATISTICS**

**Academic ⭐⭐ Business ⭐ Policy ⭐
Organised by MATIS project (BE)
Moderator Teresa Quintel, Maastricht University (NL)
Speakers Daan Vertongen, Belgian Passenger Information Unit (BE); Marianne Junger, Twente University (NL); Alexander Seger, Head of the Cybercrime Division (CoE); Michael Levi, Cardiff University (UK)

The European legislators are rapidly developing digital investigation powers of law enforcement authorities, for example the access to Passenger Name Records or the cross-border access to electronic evidence. On the other hand, the cornerstone of the Digital Single Market are new, strong and robust data protection rules, designed to strengthen the protection of fundamental rights of individuals in the Digital Age. These competing legislative developments are often implemented without objective evidence, which would justify their raison d'être. This panel should therefore explore whether we can empirically measure the use and frequency of digital investigation powers, and, based on such measurements, learn something about their fundamental rights compliance.

- What can we learn from the criminal justice statistics?
- Can we objectify the debate about the necessity and proportionality of digital investigation powers?
- Can we quantify the necessity test? What about proportionality?
- How do we ensure the tracing of the entire life cycle of personal data in the criminal justice system, from the moment of its collection/access until the end of the investigation/trial/sentencing?
Nowadays businesses are faced with an increasingly complex privacy landscape. In particular, those companies involved in international data transfers find themselves in need for more clarity and transparency of rules. Codes of conduct as co-regulatory instruments not only have an ability to react quickly to a fast-paced environment that is the current reality but also have a potential to harmonize privacy practices globally. An example of a cloud of conduct that was designed to meet these objectives is the EU Cloud Code of Conduct – the first legally operating code of conduct under art. 40 of the GDPR. During this session the representatives of the regulators, academia, and businesses will discuss in detail how code of conducts support companies in their day-to-day compliance as well as explore the advantages of co-regulatory tools and their potential to address recent challenges with international data transfers.

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

15:30 - COFFEE BREAK

16:00 - JUSTICE 3.0: AI IN AND FOR JUSTICE AND CASE-LAW AS BIG DATA CHALLENGES TO ASSIST JUSTICE, PREDICTING IT WHILE PRESERVING FUNDAMENTAL RIGHTS AND FREEDOMS

Academic ★★★ Business ★☆☆ Policy ★☆☆
Organised by Scuola Superiore Sant'Anna (IT)
Moderator Giovanni Comandé, Scuola Superiore Sant'Anna, Pisa (IT)
Speakers Thiibault Douville, Université de Caen (FR); Angelo Dali, ULMNIAI (MT); Francesca Toni, Imperial College (UK)

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

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

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

Academic ★★★ Business ★☆☆ Policy ★☆☆
Organised by Smart Global Governance / EDHEC Augmented Law Institute (FR)
Moderator Gianclaudio Malgieri, EDHREC Augmented Law Institute (FR)
Speakers Adriano Daoulisa, Smart Global Governance (FR); Ursula Pachi, BEULIC (BE); Alexandra Geeze, MEP (EU)

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

- Should the black list in the AI Act include also other AI practices (e.g., emotion recognition, commercial manipulation)?
- Should other tools protect individuals too (e.g. participatory design)? How?
- Is the proposed system of “high risk” classification effective, forward-looking and flexible enough?
- Is the AIA well-connected to other existing legal frameworks (GDPR, EU Consumer protection law)?
produced by the GDPR towards the following EU initiatives aiming to enhance fundamental rights in the new technologies.

Specific scenarios, investigated under the H2020 - VALKYRIES project as well (GA 103020676), will be discussed by the speakers, such as the development of AI solutions for first aid and multi-victim disasters, where health-related data are processed.

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

**13:00 - LUNCH**

**14:15 - ROLE OF ETHIC COMMITTEES IN THE EUROPEAN HEALTH DATA SPACE**

**Academic** ⚫ Business ⚫ Policy ⚫

**Organised by** CPME – Standing Committee of European Doctors (BE)

**Moderator** Sjaak Nouwt, KNMG (NL)

**Speakers**
- Guillaume Byk, European Commission, DG SANTE (EU); Aninka Eberstein, COCIR (BE); Otmar Kloiber, WMA (INT)

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

- How can the EHDS link clinical data and public health data to support health research and policy decision-making? How is it being done at national level?
- How will data protection be evaluated using EHDS-data? What role should there be for national data protection authorities, the EDPS or the EDPB?
- What role should ethics committees play in the future proposal for a regulation on the EHDS?
- What possible recommendations can be provided?

**15:30 - COFFEE BREAK**

**16:00 - DATA PROTECTION NEW FRONTIERS IN BRICS COUNTRIES**

**Academic** ⚫ Business ⚫ Policy ⚫

**Organised by** Center for Technology and Society at FGV/ CyberBRICS Project (BR)

**Moderator** Luca Belli, Center for Technology and Society at FGV Law School (BR/IT)

**Speakers**
- Danilo Doneda, National Council for Privacy and Data Protection (BR); Smriti Parsheera, CyberBRICS (IN); Sofia Chang, Center for Technology and Society at FGV (BR/CH); Anna Chuchrina, ABBYY (RU); Sizwe Snail, Information Regulator (SA)

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

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

**Academic** ⚫ Business ⚫ Policy ⚫

**Organised by** University of Turin, UNITO (IT)

**Moderator** Eleonora Bassi, Nexa Center for Internet and Society, The Polytechnic University of Turin (IT)

**Speakers**
- Theresa Stadler, SPRING Lab at EPFL (CH); Massimo Attoresi, EDPS (BE); Pompeu Casanovas, La Trobe University Law School (AU); Jerome Bellegarde, Apple Inc. (US)

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

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

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

in Grande Halle

---

**CPDP2022 PANELS AT AREA 42 PETITE**

**08:45 - A CYBERSECURITY INCIDENT: WHO YOU GONNA CALL?**

**Academic** ⚫ Business ⚫ Policy ⚫

**Organised by** Université du Luxembourg (LU)

**Moderators** Sandra Schmitz, SNT, Université du Luxembourg (LU); Stefan Schiffner, Westfälische Wilhelms-Universität Münster (DE)

**Speakers**
- Corinna Schulte, SAP (DE); Florian Pennings, Microsoft (BE)

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

**10:00 - COFFEE BREAK**
This panel will discuss the potential and limitations of such a calculation as well as possible approaches to its implementation. Would a surveillance calculus rather lead to a critical control or to legitimisation of (additional) surveillance measures? There are also fundamental questions: What would be an acceptable level of surveillance and who determines it?

11:45 - ACADEMIC SESSION 2

Academic Organised by CPDP

- Valeria Ferrari, University of Amsterdam (NL): The money of the present future: the platform imaginary and the empowerment/protection of consumers in EU policymaking on digital payment infrastructures
- Laima Janute, Vilnius University (LT): The right to preserve the use of cash: innovation, counter-currents, and the protection of privacy
- Ine van Zeeland, Vrije Universiteit Brussel (BE) and Jo Pierson, Vrije Universiteit Brussel (BE): Data Protection Risks in Transient Times: The Case of European Retail Banks
- Daniel Woods, University of Innsbruck (AT): Quantifying Privacy Harm via Personal Identity Insurance

13:00 - LUNCH

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

Academic Business Policy Organised by Fraunhofer ISI

Moderator: TBC

Speakers: Christian Gemini, University of Kassel (DE); Jane Kilpatrick, Statewatch (UK); Bijan Moini, GFF/EDRi (EU)

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

This panel will discuss the potential and limitations of such a calculation as well as possible approaches to its implementation. How can we record and, especially, assess the different surveillance measures of the various legislators on the EU, national, regional and local level? What would be the expected legislative effect: Would the oldest surveillance measure have to be repealed or would the latest never take effect?

There are also fundamental questions: What would be an acceptable level of surveillance and who determines it? Would a surveillance calculus rather lead to a critical control or to legitimisation of (additional) surveillance measures? What value could this debate have for the rest of the EU or even beyond? Are there any points of reference in EU law or in the constitutional law of other member states that could prescribe such a ceiling for state surveillance?

15:30 - COFFEE BREAK

16:00 - ACADEMIC SESSION 3

Academic Business Policy Organised by CPDP

- Suncana Slijepcevic, Bruno Skrinjaric and Edo Rajh, The Institute of Economics, Zagreb (HR): Citizens resilience to online privacy violation and use of digital public services
- Jorge Pereira Campos, Joao Goncalves and Jason Pridmore, Erasmus University Rotterdam (NL): Data Donation as e-Participation: How Citizens Construct the Risks of Donating Personal Data to Smart Cities

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

Academic Business Policy Organised by Georgia Institute of Technology (US)

Moderator: Peter Swire, Georgia Institute of Technology, School of Cybersecurity and Privacy (US)

Speakers: Théodore Christakis, Université Grenoble Alpes (FR); Fabian Delclos, EU Commission, DG-Justice (FR); Samm Sacks, Yale/New America (US)

What set of principles and laws should apply to government access to personal data, including for law enforcement, foreign intelligence, and national security purposes? As framework privacy and data protection laws have spread to most countries in the world, there is considerable uncertainty about how protections apply outside of the commercial sector. In democracies, state power should be exercised under the rule of law, generally including a prominent role for an independent judiciary. Non-democracies have also adopted framework data protection laws, but with uncertainty about how rule of law may apply for government actions.

China has now adopted a framework data protection law, but lacks important rule of law institutions. The United States is a democracy with law under its Constitution, but lacks a framework data protection law. Principled discussion about government access thus is emerging as central to geopolitical debates. What are the best forums for multi-lateral consideration of these issues of government access?

What is the difference between “compelled/obliged” access and “direct” access? Does this difference matter when it comes to promoting democratic principles on government access to data held by the private sector?

What legal rules and principles should apply to a democracy’s efforts to protect its national security through intelligence collection outside of its borders, including toward both allies and adversaries?

What could we learn from recent developments on these matters, including the EU/US negotiations for a successor to Privacy Shield and the OECD process following the G20 initiative for free data flows with trust?

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

in Grande Halle