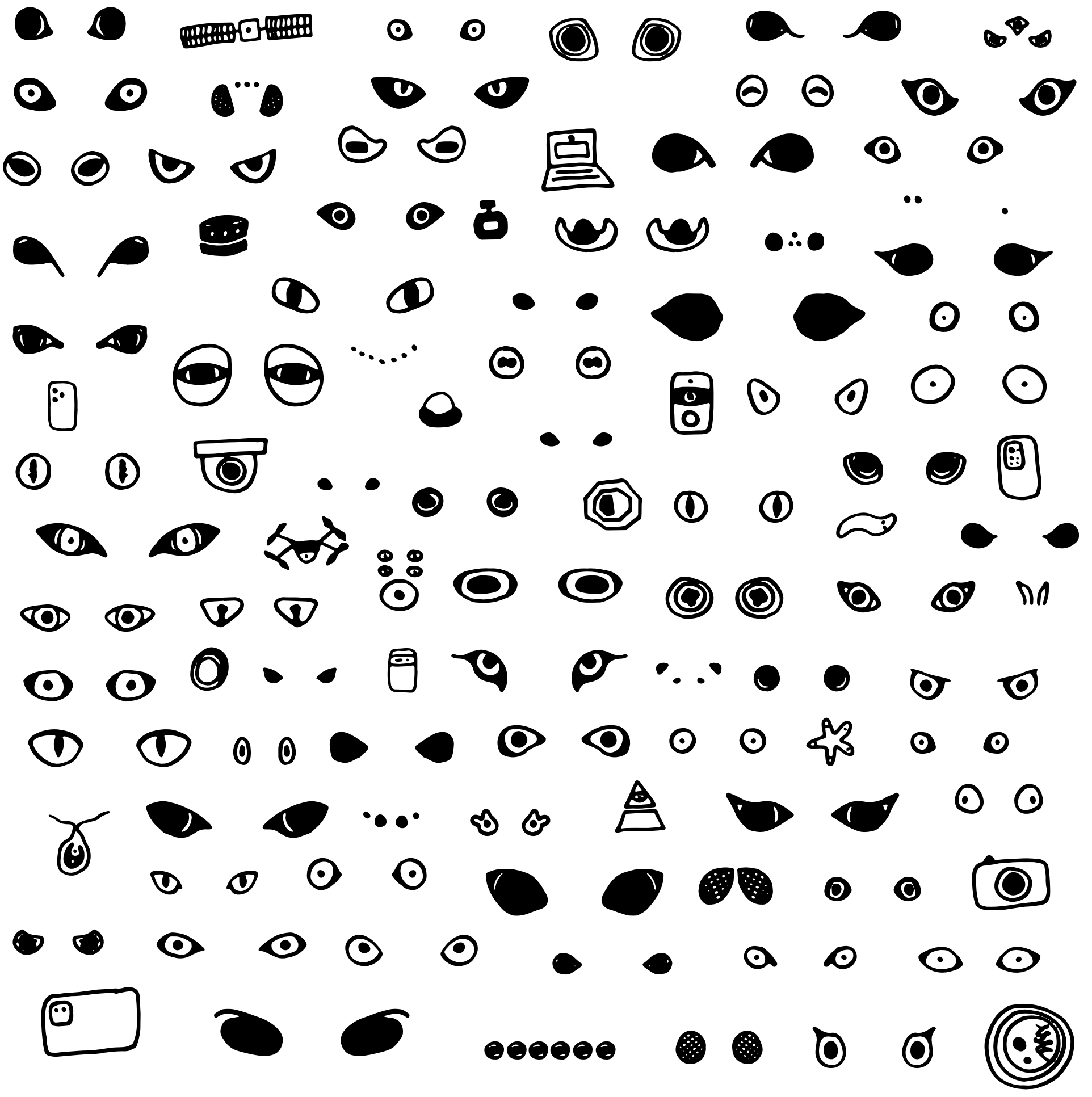
The world is watching

CPDP.ai 2025

SINCE 2007 | COMPUTERS, PRIVACY AND DATA PROTECTION | 18TH INTERNATIONAL CONFERENCE



CPDP.ai 2025

Conference Partners

ALTI

FGV DIREITO RIO

KU LEUVEN CiTiP
CENTRE FOR IT & IP LAW

CEU Universidad San Pablo

CRISP

eLAW
LEIDEN

FIZ Karlsruhe
Leibniz Institute for Information Infrastructure

Fraunhofer ISI

Georgia Tech College of Computing
School of Cybersecurity and Privacy

Inria

ivir Instituut voor Informatierecht
Institute for Information Law

dg Università di Torino
Dipartimento di Giurisprudenza

Washington University in St. Louis
The Cordell Institute

Tilt
Tilburg Institute for Law, Technology, and Society

uni.lu
UNIVERSITÉ DU LUXEMBOURG

Utrecht University

DATA SCHOOL

VUB

Dear Friends of CPDP,

Is CPDP responsive to the sense of urgency many feel about the current state of the world?

Probably not enough—but it tries. Its name ("Computers, Privacy and Data Protection")—and particularly its current form, CPDP.ai—begins and ends with a reference to technology. This reflects our belief that technology must be the subject of broad public debate—not delivered through keynotes, but explored through equal dialogue among all stakeholders. In this setting, CPDP remains committed to inclusive, multi-voiced discussions on how technology is shaping our societies, but also how our societies can shape technology. As Amandeep Singh Gill, UN Under-Secretary-General and Special Envoy for Digital and Emerging Technology, has noted: *"AI isn't just about algorithms, compute, and data. It's about power. Who has it? How is it distributed? How is it used? And how do we ensure it's used to empower people? We must prevent a world of AI haves and have-nots."*

We invite members of administrations, users of technology, and tech companies to render account for their products and practices—through dialogue with panel chairs and invited voices representing consumers and citizens: oversight bodies, NGOs, and artists. A CPDP panel has failed when its composition fails this inclusiveness. We support a model of democracy grounded in rational exploration of arguments and positions. This model does not guarantee a single answer or solution, but sees dialogue and public debate as modest ways of becoming better informed about one another's views.

The name CPDP also reflects a second core value: fundamental rights. Privacy and data protection are such rights. They may not be enshrined in every constitution, but from the far south to the deep north, they are on people's minds—alongside other human rights and lasting concerns about power imbalances. It is heartening to see the steady growth of data protection laws and AI-related regulatory initiatives around the world. In some countries, executive orders on AI usage appear and disappear in the absence of hard law. But they also return. Every political system senses that a society needs order above all, and data protection guidance contributes to that order. As a fundamental right, it fosters more rule of law quality—a third global value. Still, the global uptake of European-style data governance—often held up as a gold standard—raises new questions. Who benefits? Who is left out? The expansion of rights, however welcome, can also entrench existing imbalances if not carefully considered.

CPDP is a conference not about hope, but of hope. It is born and bred in the belief that debates—orderly but pluralistic—matter. The number of registrations this year and the organisation of the conference in a venue that allows for more and bigger panels, workshops, artist keynotes or live radio sessions, testify that this belief feels very natural for many of us. If the world is changing, let us discuss it together. If the world is watching, let them see us talk.





Paul De Hert Thierry Vandenbussche

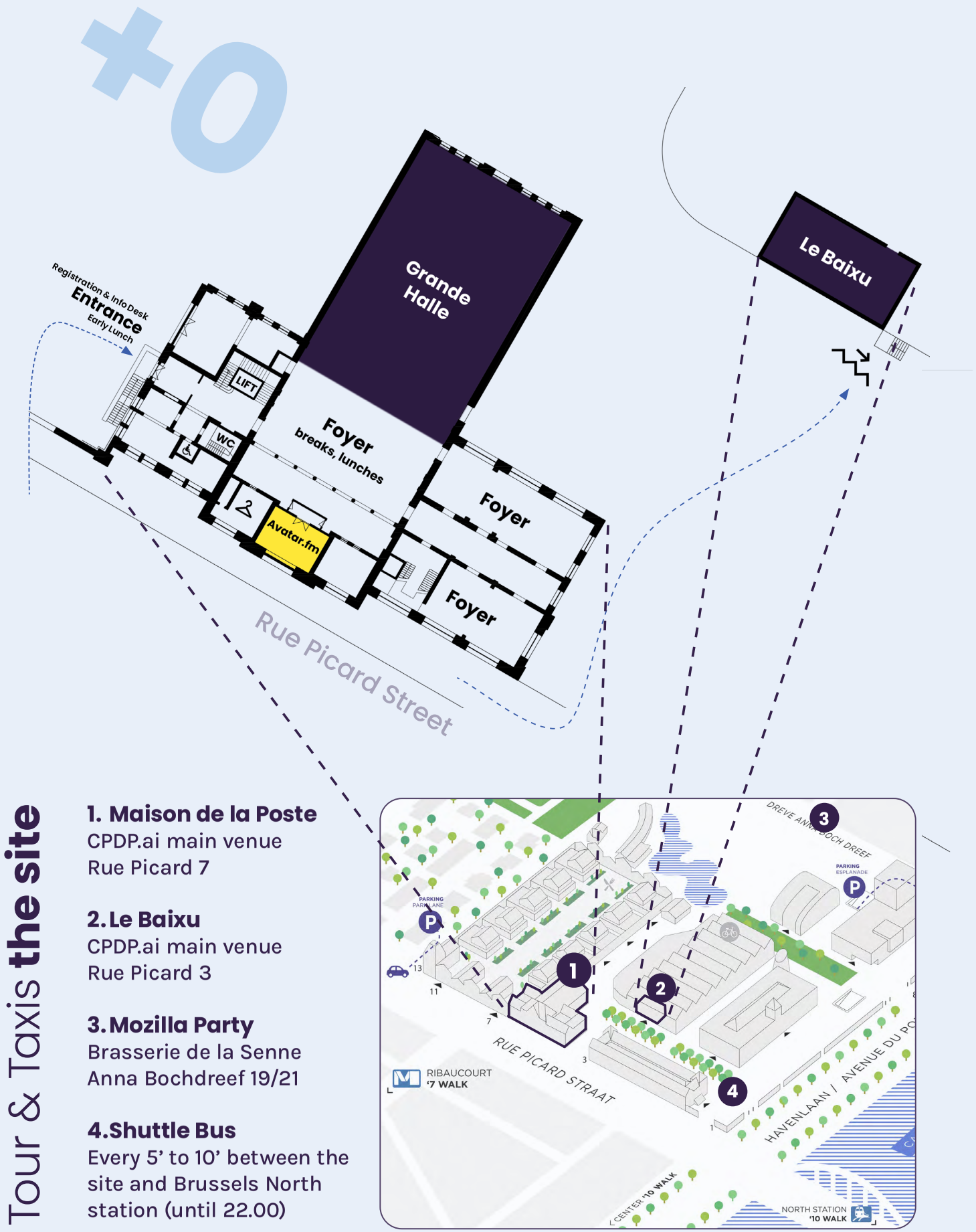
Tour & Taxis **the site**

1. Maison de la Poste
CPDP.ai main venue
Rue Picard 7

2. Le Baixu
CPDP.ai main venue
Rue Picard 3

3. Mozilla Party
Brasserie de la Senne
Anna Bochdreef 19/21

4. Shuttle Bus
Every 5' to 10' between the site and Brussels North station (until 22.00)





Panels

Workshops

Culture Club

Avatar.fm (CPDP's live radio)

CPDP.ai 2025

General Congress Information

Registration and Name Badge

Registration opens on Tuesday 20 May a 16:00 in front of Maison de la Poste, inside Gare Maritime. From Wednesday 21 May to Friday 23 May, registration opens from 7:30. You will receive a name badge with the dates of attendance.

Information Desk

We provide general information about the conference and about Brussels at the registration desk outside Maison de la Poste in Gare Maritime.

Venues

CPDP takes place simultaneously in two venues in Brussels' Tour & Taxis site. Most sessions will be held at the main venue: Maison de la Poste. Here, Grande Halle is located on the ground floor. The Maritime room is on level 1 and the Class Room and Orangerie are on level 2. All the workshops are organised at Maison de la Poste, as is the CPDP Culture Club, which can be found in the Cinema Room on the 3rd floor. Some panels take place in the revamped jazz bar Le Baixu, a stone's throw from Maison de la Poste. You can find an overview of all venue locations by consulting the map in the CPDP Magazine. You can find an overview of all venue locations by consulting the map **on page 4.**

Lunch and Coffee Breaks

All lunches and coffee breaks will be held in the foyers at Maison de la Poste and in Gare Maritime.

The early lunch will start at 12:30 outside Maison de la Poste in Gare Maritime. Regular lunch starts at 13:05 in the foyers.

Networking and Side Events

Cocktails will take place in Maison de la Poste starting around 18:40 on Wednesday, Thursday and Friday. Don't forget to check out our exciting Culture Club Programme on the 3rd floor and the Avatar.fm live radio on the ground floor.

Video Recording and Photography at CPDP

Is CPDP watching you? Well.. a bit. A professional photographer will be taking photos at the conference, including crowd shots, which may then be used for publicity. Please let us know during registration if you do not wish to be in these photographs. Panels will be filmed at the conference venue and uploaded to our archive and YouTube channel after the event (in case the speakers gave consent for the recording).

Shuttle Bus from/to Brussels North Station

A free shuttle service travels back and forth from Brussels North Station. Every 5 to 10 minutes, a bus leaves at the Tour & Taxis site or the station. Around midday, buses also go to the Rogierplein. Find the schedule by scanning the QR code.

Taxi

Please do not ask the information desk to call a taxi for you, please do this yourself. Companies like to know your name and phone number to avoid other people getting into the taxi that you booked. Taxis Verts: +32 2 349 49 49.

Updates and Conference News

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



Interview with

James Bridle

Annually CPDP is collaborating with an artist to create an image for the conference. Last year we worked with Vladan Joler. Earlier we invited David Shrigley. In 2022 we worked with the Romanian artist Taitzel Ticalos who used a sound visualisation of a CEO apologising for a data breach. In 2023 Judith Fegerl created Resistors which is a poetic proof that resistance is already inside our hardware. This year, we had the honor of James Bridle saying 'yes' to our humble request.

The theme of this year's CPDP conference is *The World Is Watching*. We see this title as multi-faceted in a time when global changes are driven by both political and corporate forces. We also consider the role of the individual, who is now more outspoken and critical. This interpretation guided our discussions as we planned our collaboration for CPDP 2025. We also focus strongly on children and their safety. How do you see this title and approach?

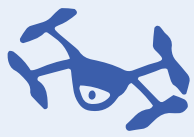
When I first heard the title, *The World Is Watching*, it took me back to over a decade ago during the Occupy Movement. I was in New York for a residency program at the tail end of Occupy Wall Street, so I witnessed the protests and encampments firsthand. *The World Is Watching* was a phrase I first encountered in this call to action for surveillance from below. Activists used it while documenting protests and exposing state violence. There was extensive surveillance of protesters, but this was a form of reverse surveillance where people filmed police actions to gather evidence of brutality and legal overreach. It felt powerful, highly networked, and deeply connected to the internet. While Occupy was a physical presence, it was also an online movement, broadcasting itself through countless networked cameras. The iconic image of people holding up their phones to livestream felt like a new kind of media event, a fusion of digital and physical space. Since then, the idea of *The World Is Watching* has expanded, as has surveillance itself. There's the spread of CCTV cameras, online tracking, and the accumulation of data by corporations. This extends into what Shoshana Zuboff called *surveillance capitalism*: an economic model built entirely on watching and tracking. For me, the phrase has a dual nature. It implies citizen activism, looking back at power and spreading information, but it's also tied to the rise of state and corporate surveillance, creating a kind of panopticon around us. I have complex feelings about this, especially because my own work has examined surveillance extensively. I've studied state and corporate surveillance, created artworks about it, and written extensively on the topic. But over time, I realised that much of the criticism of surveillance (whether in writing, art, or activism) tended to reinforce the logic of surveillance itself. Many critiques relied on conducting even more surveillance to expose the issue, ultimately just generating more data and desensitising people. When you repeatedly tell people they are being watched, the response is often fear, paralysis, or disengagement. It creates a cycle where surveillance and resistance exist in parallel but remain trapped in the same logic. Another area I explored, which ties into your theme, was children's activity online. At the time, I wasn't a parent, but now I am, and my perspective has evolved. I grew up with the internet, having unsupervised access from the age of 12. I saw things I shouldn't have, engaged in practices I wouldn't want a child to experience, and yet, I also credit much of my development to that early digital freedom. Many people of my generation share this paradoxical experience—we were exposed to harmful content, but the internet also shaped who we are. I wrote an essay, *Something Is Wrong on the Internet*, examining how online platforms exploit attention for profit, often at the expense of children. Large corporations prioritize revenue over safety, leading to deeply disturbing consequences. The reports I uncovered described severe trauma, yet these companies largely ignore the harm they facilitate.

Your artwork for CPDP clearly explores the more-than-human world and our shared existence within it. In the context of regulation and policy discourse, this brings us to legal frameworks like the 'rights of nature.' How do you think acknowledging a more-than-human web of perception could impact our European approach to regulation?

Over the last few years, my work has shifted—not away from technology, but toward a broader ecological perspective that includes the more-than-human world. This means considering non-human beings in all their forms and redefining what matters when we talk about perception and awareness. When I reflect on the phrase *The World Is Watching*, I ask: who do we mean by "the world"? Much of my work on the non-human world has focused on perception, which is a fascinating way to explore this concept. The more-than-human world consists of all beings that inhabit it, and understanding it through perception raises fundamental questions: Who sees? How do they see? What perceptions do we share? In responding to this theme, I became interested in the idea of all these watching eyes, quite literally, the eyes of many different beings observing the world. This includes humans, but also non-human animals in various forms. It even extends to unexpected forms of perception, such as the sensory systems of plants, which perceive light in specific ways. It also includes technological systems such as CCTV cameras, doorbell cameras, and surveillance systems on military drones. I wanted to create a broad mapping of all these different systems of perception, these various ways of seeing, that collectively form a world that is watching, and is thus capable of acting in response.

You've talked about Richardson's paradox, which suggests that the more we measure the world, the more complex it becomes. Regulation follows a similar pattern: the more we regulate, the more complex it gets. When including non-human species in regulation, this paradox seems inevitable. How do you reflect on this?

I've long admired Lewis Fry Richardson. He was a meteorologist who developed weather prediction by numerical calculation, the foundation of modern forecasting.



When you repeatedly tell people they are being watched, the response is often fear, paralysis, or disengagement. It creates a cycle where surveillance and resistance exist in parallel but remain trapped in the same logic.



UAV Identification Kit 001", 2012, pelican case and 3D printed models

His work parallels the rise of computation through gathering data, mapping it, and predicting the future. This connects to surveillance, as prediction is ultimately about control, whether for weather or for social, political, and economic data. Richardson was also a Quaker and pacifist. He served as a stretcher-bearer in World War I, refusing to fight, and resigned from the British weather service [Meteorological Office] when it became militarised. Instead, he studied peace, hypothesising that conflict likelihood correlated with border length. But in measuring borders, he found they were fractal. This illustrates a broader truth: more data doesn't always mean more understanding. The assumption that studying something in finer detail leads to greater knowledge, and ultimately control, breaks down. There's a limit to what we can know, especially about non-human beings. The scientific method, while valuable, is not the only way to understand the world. Richardson's paradox reminds us that alternative ways of knowing are essential. It also highlights the need for moral and ethical considerations. His science was inseparable from his pacifism, anti-militarism, and rejection of imperialism. When engaging with his ideas, we must ask: What moral stance do we bring? What kind of world do we want to create? These questions should shape our approach from the start.

You previously talked about shifting our perspective on AI as a servant to AI more as a colleague. What do you think is necessary to put this paradigm shift into motion to get from that place to AI as a colleague?

Conversations about AI are fraught because we're always discussing both the popular imagination of AI and AI that actually exists. The former is shaped by narratives of superintelligence, an omnipotent mind emerging from nowhere. But in reality, AI is just statistical models working with vast amounts of data. I studied AI academically 20 years ago, during a lull in its development. The current wave isn't based on a conceptual breakthrough because neural networks existed then. What changed is society: corporate power, data accumulation, and computing resources have exploded, allowing AI to scale. But today's AI, shaped by surveillance capitalism, serves corporate interests. Its primary function isn't generating images, text, or code—it's making money. This is what I call corporate intelligence. Like corporations, AI enables various tasks, but everything ultimately serves profit. If we work with AI, we're always operating within that structure. To truly see AI as a colleague – or better, comrade - we need a different model, both in how we create and experience it. That requires rethinking not just AI but our entire social and economic systems. AI is often framed in human terms, but intelligence isn't uniquely human. It arises from being in the world, shaped by form and context. Human, non-human, and machine intelligences are distinct. To engage meaningfully with AI, we must examine who controls it and who dictates its purpose.

It's often said that regulation lags behind technology, but couldn't this be seen as part of the natural flow of development? From your perspective as an artist and researcher, how have you seen digital regulation evolve? Is it strengthening or weakening in today's changing world?

I'm not a policy expert, but the idea that regulation *must* lag behind technology is a weak excuse for inaction. We *can* anticipate and react to developments, and there's no reason not to legislate just because technology moves fast. Societies choose how they want to be governed, and we've seen effective legislation, like the right to be forgotten, GDPR, and Freedom of Information, despite their fragility. These laws are under pressure, especially in the US, but that doesn't mean they aren't worth defending. Europe seems more committed to these efforts. At the same time, I'm wary of state regulation. In the UK and US, many online regulations stem from moral panics, often harming marginalised groups under the premise of protecting children. Governments tend to use technology regulation regressively, targeting minorities rather than addressing real issues. So while legislation has its place, it's not the only answer. The real solution is education, social change, and systems that are transparent and user-controlled. The need for state regulation of transnational corporations diminishes when we have more direct control over the technologies we use.

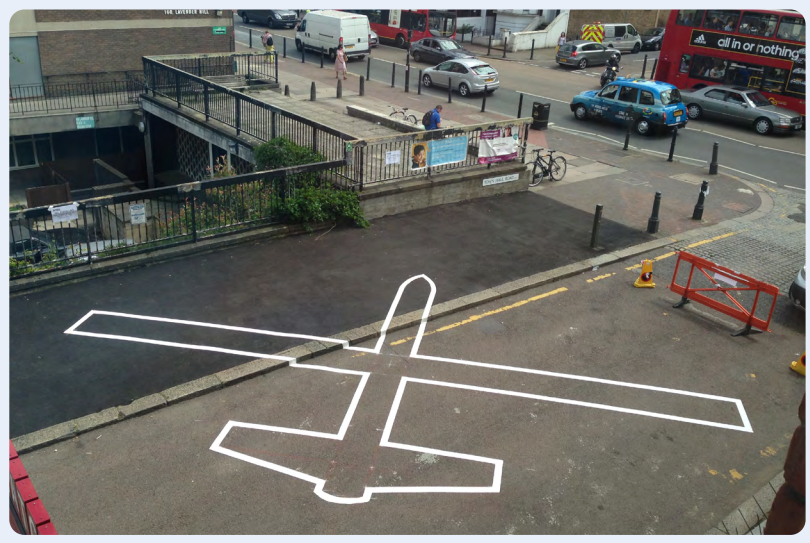
Children have long been exposed to autoplay features on various platforms, often leading them to strange and unsafe content. Despite new platforms emerging, lessons from past ones haven't been applied to improve child safety. Regulation is always playing catch-up, but do you think there are lessons that could be learned and implemented?

The first thing to say is that big corporations claiming to protect children are lying. We've seen this repeatedly. Take YouTube Kids, for example. It claims to be safe, but it isn't. At the scale these platforms operate, proper moderation simply isn't possible. It's physically, technologically, and mentally unfeasible. Any claim that they can provide safe moderation for children is false. Beyond that, these companies have no real incentive to fix the issue. Their business model depends on making content as accessible as possible, so restricting it is an existential threat to them. Safe platforms for kids do exist, but they don't scale in the same way or generate as much profit. That doesn't mean we can't choose them—it just means they're not prioritized. Stepping back, my position is simple: no child should have unmoderated access to media. That's not a technological problem; it's a social one. It comes down to education and childcare. As any parent knows, children spend excessive time online because parents are busy and need to occupy them. The real issue is that childcare is inadequate, and parenting is often too isolated. The nuclear family model in the West simply isn't enough—we should be raising children as communities. So while we can say children shouldn't have unmoderated internet access, enforcing that is another matter. The root causes are much larger social issues. If we address those, we'll naturally solve many of the technological concerns as well.

Your books have been a major inspiration for many interested in the digital world and its societal impact. What are you currently working on? Can we expect a new book, or are you focusing more on exhibitions—or maybe both?

There's always more coming. My work emerges from what I'm drawn to, and I've noticed a growing practicality in my approach. While writing *New Dark Age*, I explored the relationship between technology and climate, both the harm technology causes and the impact of climate change on technological systems. Confronting the reality of climate change was terrifying and sent me into a deep depression, something many readers also expressed. That led to *Ways of Being*, where I expanded my thinking to include ecological technologies. This ranged from high-tech solutions like solar panels and smart grids to low-tech approaches like permaculture and traditional knowledge systems. The more I engaged practically, such as learning to wire a solar panel or plant a permaculture garden, the more my depression lifted. The biggest fear was feeling powerless, and action restored a sense of agency. This powerlessness extends beyond climate change. It defines our relationship with technology, politics, and finance, which fuels populism, fear, and inaction. Agency is the ability to act, to have a place in the world. That's what I'm interested in now: increasing agency through renewable energy, alternative democracy, water and soil management—practical skills that reconnect us to the world. No single solution will save us. Solar panels alone aren't enough, but they're better than fossil fuels. The key is engagement, or learning by doing. This applies to everything: coding, carpentry, gardening. We need diverse intelligences working together, not knowledge concentrated in a few hands. A system where only a small group understands how things work leads to power imbalances. Education must be both broad and deeply practical. In learning to make and build, we develop the solutions we don't yet know we need. ▪

To truly see AI as a colleague – or better, comrade - we need a different model, both in how we create and experience it. That requires rethinking not just AI but our entire social and economic systems.



Drone Shadow 007: The Lavender Hill Drone, 2014, installation, London

DPO Track

CPDP Shines a Spotlight on the Role of the DPO

OPINION PIECE

At the 2025 CPDP Conference, the role of the Data Protection Officer (DPO) takes center stage. For the first time, a dedicated DPO track has been included in the programme, ensuring DPOs get even more value out of the conference. We spoke with Jolien Ghyselinck and Peter Berghmans, the curators of this new track, who emphasized the need for a broad, international dialogue around the evolving role of the DPO. CPDP.ai invited the curators for an opinion piece where they emphasise the need for a broad, international dialogue around the evolving role of the DPO.

Computer Science and Data Protection Officer Tracks

As a novelty at CPDP.ai, this year's edition features two "dedicated tracks". Join us on Wednesday to engage in multidisciplinary debates around computer science topics. On Thursday, data protection officers and other privacy professionals get together to discuss subjects of particular interest to data protection officers, and the challenges and opportunities that these professionals face in an evolving digital landscape. Curated by experts with a strong grounding in these subjects, the dedicated tracks aim to nurture interdisciplinary discussions and connections amongst specialists and with the wider CPDP community.

Unsurprisingly, the changing nature of the DPO's roleis a hot topic. Legally speaking, nothing has changed—the GDPR still defines the DPO's core responsibilities. "But in practice, governments and companies are increasingly turning to their DPOs when it comes to interpreting new European tech regulations, especially the AI Act," states Jolien. That brings us to the buzzword of the moment: artificial intelligence. Many organisations are exploring the opportunities AI presents while grappling with the legal boundaries. "I'm not sure whether this shift is good or bad for the DPO," Jolien observes. "On the one hand, it allows DPOs to contribute to technological innovation. On the other hand, it risks compromising the DPO's independence."

Jolien refers to prior research conducted in Belgium, which revealed that DPOs often struggle with limited budgets, time, and training. "If they're asked to focus on other areas without receiving additional resources, there's a real risk that data protection might lose its important place on the agenda. While new legal frameworks can be interesting for DPOs and offer chances to specialise in other areas, this shouldn't come at the expense of their core mission."

"That's why this conference will focus on the DPO's essential tasks," Peter clarifies. "The topics are highly relevant and zoom in on the legal and practical challenges DPOs face in today's data protection landscape. My motivation for curating the DPO track is to bring the DPO's role, position, and responsibilities to the forefront of academic and professional discussion—and CPDP is the ideal platform to do just that." Jolien adds: "For me CPDP is also a great platform to stimulate the dialogue between DPOs and the business world by building bridges between the theory and the practice".

The curators have been working passionately over the past few months to shape this track. With 3 panels and 3 workshops, a full day is dedicated to DPOs. One highlight is the panel titled *The DPO Universales: Crossing Borders on a Bumpy Road*, developed in collaboration with Simon Hania from Uber. "This panel will explore the challenges DPOs face when navigating the diverse roles assigned to them under international data protection laws," Peter and Jolien describe.

Furthermore, supervisory authorities and the EDPB are actively participating. "Their involvement is crucial to the success of the DPO track and we are happy that the practical side is integrated, for example in the workshops," the curators note. Previous research on DPO happiness in Belgium showed that the relationship between DPOs and the supervisory authorities is not always optimal. This year's program aims to address that gap with, among others, an EDPB cookie workshop, a CNIL panel on The Economic Benefits of Having a DPO, and a workshop by the Flemish supervisory authority exploring connections between DPOs and regulators. Sector-specific challenges are as well on the agenda, such as the EDEN panel on Data Protection for European Law Enforcement.

By bringing DPOs together at CPDP, the conference gains an extra layer of depth—one that will hopefully continue in the years to come. Jolien and Peter point out: "We are very grateful that a discount of 50% was given to the DPO's and privacy professionals for the day ticket of the DPO track. 👁 👁 This is an inclusive approach to help them find the way to CPDP, because unfortunately not all of the DPO's and privacy professionals have enough budget to maintain their expert knowledge".The curators have also launched an international version of their DPO Happiness research. "We want to identify the key success factors that make DPOs thrive in their roles," they explain. "These insights help us open up relevant discussions with an international and diverse audience." ▪

Peter Berghmans and Jolien Ghyselinck, DPO Track Curators

Peter Berghmans is a member of the Flemish Data Protection Authority and CEO of the Data Protection Institute. He is a Data Protection Officer in the healthcare sector and lectures on Data Protection at Thomas More University of Applied Sciences. As a co-curator at CPDP, he highlights the crucial role of the DPO.

Jolien Ghyselinck is DPO at the National Institute for Criminalistics and Criminology (NICC) in Belgium and appointed for data protection of DNA analysis in criminal matter (public sector). She is also a board member of dpo pro, Professional Union of Data Protection Officers in Belgium. From her own experience she believes that supporting DPO's from different angles is very important, that's why she is also co-curating the DPO Track at CPDP.ai 2025.

Are you a DPO and interested in contributing to the research?

Fill out the survey here ⟶

thomasmore.questionpro.eu/DPO2025

CPDP.ai 2025

CPDP CULTURE CLUB

Cinema • 3rd Floor

08.45 -18.45

Deep within the impressive architecture of our conference location, we run a programme called the CPDP Culture Club. It is a temporary sanctuary - if you like - to take a break and immerse yourself in a programme of art, books, films, talks, and coffee, all carefully interwoven with the main programme.

DAY 1

TUE 21

Aaajiao • Frederik De Wilde • Natalie Smuha • Aurelia Tamò-Larrieux Francien Dechesne • Konrad Kollnig • YAO Qingmei • Dahai Zhang Jiao Feng • Sejal Shah • Clarisa Sánchez Gutiérrez • Thaïs Baert Anastasia Siapka

DAY 2

THUR 22

Marietje Schaake • Paul De Hert • Irene Kamara • Esther Keymolen Matt Mahmoudi • Petra Molnar • Alessandra Calvi • Laurence Meyer CODE 2025 • Boris Shershenkov • Maria Magierska • Global Witness

DAY 3

FRI 23

Daniel J. Solove • Damian Clifford • Laura Drechsler Eduard Fosch-Villaronga • Gloria Gonzélez-Fuster Anastasia Karagianni • Chris Hables Gray • Dimitris Bouris • Hourya Bentouhami • etc

MORE INFO: **CPDPCONFERENCES.ORG**

Sponsored by Mozilla

CPDP's Official Party

Thursday 22 May, 20:30 PM

Brasserie de la Senne, Anna Bochdreef 19–21, 1000 Bruxelles

Join us for drinks, nibbles, and a chance to connect with others building a better digital future for all.

TACTICAL TECH

CPDP.ai 2025

DATA DETOX

BAR

AI EDITION

The Data Detox Bar is a meeting point where you can take control of your data privacy, digital security, and online wellbeing. You are invited to think about digital topics in an analogue space, creating a truly unique experience. Staying true to its forerunner the Data Detox Kit, the Data Detox Bar provides a variety of simple and non-judgmental tips and tricks to help visitors navigate tech more confidently.

Maison de la Poste
second floor





Exhibition view | Photo by Michele Margot

Back to Feelings Inc.

OPINION PIECE

Let's take a moment to look back and take a walk through a by now memorised and archived *Feelings Inc*: A Privacy Salon exhibition that attempted to navigate the delicate interplay of vulnerability and connection in online matchmaking, digital companionship and beyond. It housed an international selection of artists that span different generations - from the very now to historical perspectives about our emotional bonds with the algorithm.

As we entered the exhibition we stepped into the hyper-feminine universe of Arvida Byström, immediately embracing the role of social media and its sexualization of feminine bodies. Arvida's work challenges the use of artificial intelligence, with the inherent social biases of its driving algorithms. A 4-meter high and 5-meter-wide body fills the spectators' field of view. Its limbs and head nowhere to be found. Berlinde de Bruyckere on AI, exposing the algorithm's biases...

As our vision breathes again, our eye caught 8 high-tech cradles each carrying an artificial uterus. Wired with umbilical-like cords they seemed to transfer some strange marriage between data transfers and bodily fluids. Marie Munk's uncanny visual language challenges normative notions of the biological human being at a time when technological innovation mingles with the fostering of intimate and sexual relationships.

Above this bizarre mix of delivery room and data center floated a neon pickup line by artist duo !Mediengruppe Bitnik: 'Is anybody home lol?' As a remnant of the Ashley Madison data breach, it pointed at the disproportionate deployment of female bots behind online dating platforms. Married men were cheating on their wives with robots, without their knowledge.

Within the white cube, a black server-like structure housed two films. One of them following Ariane Loze who impersonates multiple characters (several app users, app voices, CEO's...) wandering the streets of a science-fictional Paris. Addressing the camera, the characters reveal how our data is exchanged and sold without our knowledge when being (non-) active on social media and dating platforms.

The other film, accessible on the other side of the black box, told the story of Replika chat bots, designed to replace us after our death for our loved ones. Its goal is to learn as much as possible about us to reproduce an identical self. Inès Sieulle's film '*The Oasis I Deserve*' captures conversations between humans and Replikas, navigating our relationship to the unkown or even the shared violence it produces.

By opening the black box of Replika, we enter the latent space of Large Language Models (LLM's) where language drives human-machine intimacy. The collaborative project '*Latent Intimacies*' gestured to AI's potential for alternative forms of intimacy, existing inside the latent space of low-tech language models. Three prototypes echoed the semantic accidents captured in earlier, more primitive human-machine interactions. With these Vytas Jankauskas and his collaborators hint at new possibilities for human-machine connection.

Moving beyond human-machine intimacy, Lawrence Lek's Guanyin told the story of a Carebot, a cyborg therapist created to save other AI from the brink of self-destruction. The work is a game. It allowed us to wander around an open world where players take on the role of the Carebot as they try to stop a self-driving car from destroying themselves.

While the concepts of chatbots, virtual companionship and caring robots may feel new, they are not. Since



Installation view from Marie Munk | Photo by Michele Margot



Installation view from Lynn Hershman Leeson | Photo by Michele Margot

the 1960s, Lynn Hershman Leeson has been experimenting with new technologies and the potential of cyborgs, engaging with the urgent issues of gender, privacy, surveillance, and censorship. In her short video *Seduction of a Cyborg (1994)*, technology is illustrated as an infectious disease that destroys a woman's immune system.

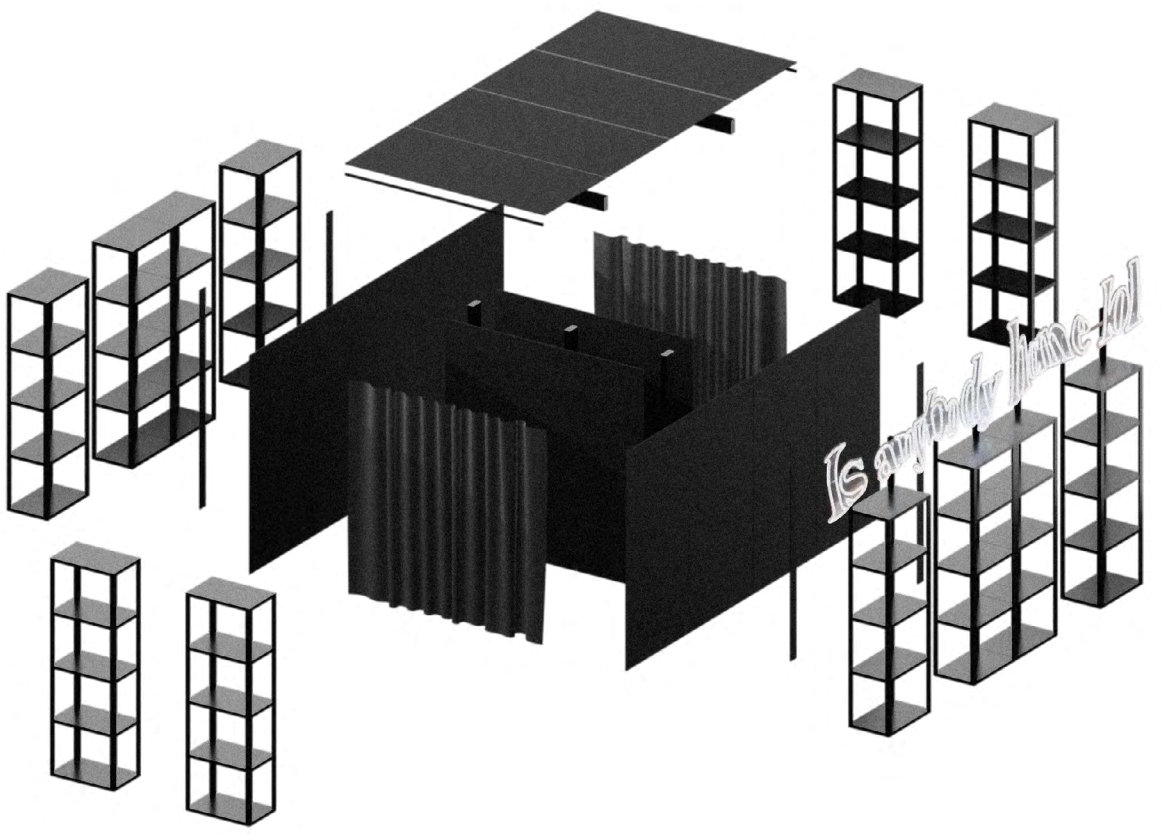
Around the same period Olga Morano subverted the masculinity of algorithms, by reproducing the mathematical figures from her husband's physics books with humor and sensuality on a canvas.

We end our journey in outerspace. Paul Van Hoeydonck is the artist whose sculpture joined one of the early Apollo flights. It is known as the only artwork on the moon, so far. In the 60's he worked on series like Homo Cyberneticum, visualising his futuristic and romantic ideas about the intersection of humans and machines.

Feelings Inc. does not take an explicit position for or against the right or possibility to have a certain emotional relationship with a non-human (machine). Rather, it tried to form an opinion about the possible polarising effects that this could trigger. It attemped to understand the meaning and implications of individualisation that is developed through exponential usage and normalisation of non-human (machine) relationships. Its focus extended beyond dating apps to include embodied AI chatbots like Replika, where people fall in love with an avatar created by Luka inc. The user can experience emotional loss when the newest update caused a data loss...

This exhibition was on view early 2025 in Huidenclub Rotterdam. On valentine's day a two-day symposium allowed a handful of experts, artists and civilians to dig deeper into the topics touched upon by the presented artworks. These were all recorded and archived on Privacy Salon's Youtube channel, and you are very welcome to relive every moment! ▪

Ferre Vander Elst



Computer Science Track



Interview with

Jaap-Henk Hoepman

Jaap-Henk Hoepman is co-curator (with Marit Hansen) of this year's CPDP Computer Science Track. He is an associate professor at the Digital Security group of the Radboud University, Nijmegen, and a principal scientist (and former scientific director and co-founder) of the Privacy & Identity Lab. In October 2021 his book Privacy Is Hard and Seven Other Myths. Achieving Privacy through Careful Design appeared at MIT Press.

You are known to many people in the CPDP community, but could you share a few words about yourself, your work, your relationship to CPDP?

I think I'm a long time participant at the CPDP, to be honest. I don't even remember when my first time was. It might easily have been 15 years ago, if that's how long CPDP exists. I don't know. And I've always gone because it's such a nice mix of policy people, lawyers and also a little bit of computer scientists, but not so many – all of which work on data protection and privacy from all across the world. And yeah, for me that's super interesting because I'm a computer scientist working in privacy, privacy by design, privacy enhancing technologies. I like to work on problems that are inspired by practice. This is a good source of new problems, new issues.

For this year's edition, CPDP is grateful that you are co-curating the computer science track. How do you see this and what would be a good outcome of this track?

We don't have a lot of experience yet. I mean, it's like an experiment. The idea was to maybe attract more computer scientists to CPDP because there's few of them compared to other "factions" or how you want to call them. There are not many and it would be good if there are more. Let's see if that happens. So to say whether the experiment was successful or not is something that I can only answer after CPDP, I guess. For me, the main thing is seeing more fellow computer scientists, then it will have been good.

Why do you think CPDP is a good platform for computer scientists to get together?

Well, CPDP will be an awful platform for computer scientists to get together with only computer scientists. But that's not the point. The point is that they get together with policy people, lawmakers, legal scholars, … That's the whole point. And CPDP is a very good venue for that. I've always enjoyed it, and I think for many computer scientists it's relatively unknown, and therefore we are trying this to get them involved.

On a general level, how do computer scientists benefit from more interaction with legal and policy experts?

On several levels. I think in general there is a significant number of computer scientists working in data protection and privacy who don't necessarily have a very good understanding of the more social and the more legal aspects of it, which means that if they think about solutions from their discipline, they may sometimes solve the wrong problem. Or they may solve a problem in the wrong way, because they're not really accounting for the social and legal dimension. So that is one reason why it is important, and the other thing is that, sometimes from a computer science perspective, there's not a problem at all, but then, from a legal perspective, there is. So, you might think as a computer scientist that you've completely solved the problem, but it's not solved. This, in general, depends a bit on the kind of computer scientist that you are, but if you want to make your work more relevant, it is nice to get inspired by actual problems that occur in practice. There are many ways that you can get inspired by problems that happen in practice. You might work with companies, you might engage with civil society, or you can go through other disciplines to see how they look at this problem and get inspired.

Let us turn to a technical topic – the local processing of personal data, which is becoming quite important in the age of AI. As you mentioned in your book ("Privacy is Hard and Seven Other Myths"), iPhones have been doing it, and now Microsoft Copilot is doing it. How do you feel about this way of processing personal data? Does it provide adequate privacy guarantees?

Local processing in general is a way to protect privacy because it means indeed that your specific data does not leave your own device and therefore does not risk being abused by any third party, which is of course one of the reasons why we want to have privacy and data protection.

The example I give in my book is the example of Apple allowing you to search only on your device for pictures which happen to have a certain face. In that case, that specific application is clearly for your own benefit. You want to have photo albums categorised based on the people on the pictures and that's it. But more and more of the local processing is done through



In general there is a significant number of computer scientists working in data protection and privacy who don't necessarily have a very good understanding of the more social and the more legal aspects of it, which means that if they think about solutions from their discipline, they may sometimes solve the wrong problem. Or they may solve a problem in the wrong way, because they're not really accounting for the social and legal dimension.

things called federated learning. What the system tries to do then is to observe your local behaviour, to derive certain information about you and to collectively construct a model about, let's say, the typical behaviour of Northwestern Europeans regarding the use of Signal. You can do all kinds of trainings or [find out] which kind of words or emojis are most popular. That kind of stuff. And so that data is then fed into a model that is then actually used by those companies for all kinds of purposes that might be harmful to us as individuals or to society. Then you would say, strictly speaking, privacy is protected and there's this concept of differential privacy where mathematically speaking (and you can have debates on how good the protection actually is), but the idea is that the system that you built, and the analysis that you get out of that system, is such that you can actually prove that it doesn't matter that your personal data is in or is out of that dataset being used to answer the question. That means that, strictly speaking, your privacy is protected because it doesn't matter that you are being interviewed or not, but again, collective inferences can be made that have an impact on society and have an impact on you individually.

The last paragraph of your book says: "Significantly improving the privacy of the apps and services we use should be our first priority. But at some point, we need to dig deeper down into the technology stack and reconsider the designs for our computers and networks, both at the hardware and the operating system levels. These designs are half a century old by now and never fundamentally changed, while the world in which they are used has changed beyond recognition. We are stretching the boundaries of their use beyond the breaking point – not only in terms of privacy but also in terms of security and reliability. It's time to start redoing the plumbing, instead of applying Band-Aids to temporarily stop some leakage while we frantically mop the floor against all odds." The world has continued to change in the few years since you wrote these words – has technology and privacy by design caught up a bit, or started to catch up?

Perhaps a little bit at the highest layers of the stacks, in terms of things like federated learning, but less if you look at the lower layers of the stack. Take for example the results of a seminar I was at last week, where people were presenting about how home automation works. You have these home automation devices, more and more of which get introduced into our homes – light bulbs, voice assistants, TVs, everything is smart these days. It turns out that these devices are programmed in such a way that they constantly communicate to get, for instance, in touch with devices that are useful to them, so they can e.g. provide services together. This leaves lots of traces that you could pick up if you wanted to. Now it turns out (and I was surprised about this), that there's quite a few software development kits that are embedded in software that people write that can actively try to obtain that information. That basically means that, if I'm using a phone and I would have some of these applications with these software development kits installed on my phone, then my phone will be spying on my home to see what kind of Internet of Things devices are in my home, or if I'm somewhere else, what kind of IoT devices are in the other place. So, it turns out that things like browser fingerprinting, which was restricted to browsers, which is bad enough, is now sort of expanding to physical fingerprinting – what devices are in this space? And of course, everybody has a different set of devices, which is a unique fingerprint, and it tells a lot about the kinds of stuff that you have and do. In that sense it's getting worse, because more and more of this technology gets sort of embedded into our daily lives, and this was the promise of the ubiquitous computing, the computing disappearing in the background. But it is not disappearing for anybody who is listening to all the signals and things that they are doing to do so. And in that sense, it is not getting better at all.

Can you tell us a bit about the projects that you are working on now?

I have been quite busy with the whole European identity wallet developments as eIDAS2.0 got accepted. This is a nice topic for CPDP. Sometimes I jokingly say that I am a computer scientist that reads regulations for breakfast. It is important as a computer scientist to read these things and to engage with them because if you read the regulations, they are full of nice promises of how important privacy is. Super, that's excellent, but the actual privacy properties of something like the European identity wallet are only defined by the actual implementation of these wallets, and the problem is that you cannot in any legal language describe how such a system should work to ensure that it satisfies the properties that you want. The actual regulation tries very hard to do that, but it fails, and it's not the fault of anybody, it's just that you cannot do it. Legal language is not precise enough to do that. This means that you must engage with the thing that defines and specifies the European identity wallet and that has a very strong impact on the security, privacy, trustworthiness of the overall system (in this case it's called the Architecture Reference Framework). And that means that the writing, the development of that specification should be given the same political deliberations as the legal texts do, and I know for a fact that certain members of parliament at the time expressed concerns about the fact that they could only debate the regulation text, but not the technical specifications. Now whether they are competent enough to discuss and decide the technical documents is another discussion, but you see there that it is important to also have computer scientists, but also civil society more onboard when these technical standards are being challenged. CPDP is a nice platform to talk about these things, why they are important, but the incentives are not very well aligned. It is hard to get a computer scientist, or civil society on board because it takes a lot of time. Civil society doesn't have a lot of money; computer scientists maybe do but I mean they are academics in general, we don't get rewarded for that kind of work.

Lately, I'm thinking more about the question of the difference between the digital and the old physical world in terms of disruptive power of the (let's say) "non-discreteness" of the digital world, meaning that in the digital world, you may spend a lot of money developing a service but once it is developed, you can scale it almost for free. And in that sense, maybe it's relevant to the theme "The World is Watching" because this has tremendous impact on surveillance powers, so states can invest research in order to develop surveillance tools and once the tool for surveillance is out there, it scales to millions, billions of people, whereas in the traditional world, if you wanted to surveil people, you would have to have real human agents to do that. If you want to surveil 10 people day and night, you will have to have 30 agents to do the surveillance in shifts. At some point you must decide because you don't have that many agents. You must decide, I'm going to watch that guy, and not that person, because you don't have that many agents out there. In the digital world it doesn't work that way, you can very easily with the same amount of effort needed surveil 10 people or surveil a billion people. The effort is roughly the same. And this is a concern, it makes the whole debate about privacy vs. security very binary in the sense that either you have full privacy, or you have full surveillance, there is nothing in between. It makes the discussion very complex. I am trying to think of ways that you can add friction to surveillance tools so that you can guarantee a tool never scales to surveillance of a million people, because you would have to spend a lot of actual physical resources to do that. Similar things could also be very interesting to study, like the spread of fake news, or the first mover advantage, where the first person to have a big share of a specific market is the one that's going to dominate the market, who is going to have the monopoly, Because nobody else can actually enter the market anymore. Maybe friction there can also help us. This is a very speculative area of research that I now only started to think about. ▪



The problem is that you cannot in any legal language describe how such a system should work to ensure that it satisfies the properties that you want... And that means that the writing, the development of that specification should be given the same political deliberations as the legal texts do...

Computer Science and Data Protection Officer Tracks

As a novelty at CPDP.ai, this year's edition features two "dedicated tracks". Join us on Wednesday to engage in multidisciplinary debates around computer science topics. On Thursday, data protection officers and other privacy professionals get together to discuss subjects of particular interest to data protection officers, and the challenges and opportunities that these professionals face in an evolving digital landscape. Curated by experts with a strong grounding in these subjects, the dedicated tracks aim to nurture interdisciplinary discussions and connections amongst specialists and with the wider CPDP community.

The Governments are Watching, and So Are We

OPINION PIECE

The Governments are Watching, and So Are We

It was fall 2018, when I first entered the US academic world. I had arrived at a university in Michigan, I was a fourth-year undergraduate student, finalising my Bachelor's in Political Science and Psychology as a student on a J1-Visa.

During that time, conflicts around the world, where my passion… Yeah I know it sounds macabre, but I had spent enough time working with the Heidelberg Institute for International Conflict Research on understanding international politics and conflicts, driven by the hope that one day we might find solutions to conflicts older than me, older than my parents, and even older than some governments.

It was during that year that I was writing my thesis on nothing more ironic than "Alliance Theory" in International Relations… You can guess which alliances I was looking at. With that in mind, I enrolled in historyclasses intending to refresh my knowledge before diving into the depth of thesis research. Instead, I encountered professors who opened entirely new doors for me: Doors that exposed me to histories and narratives never taught to me in Germany. This one year allowed me to form an educated opinion on conflicts I once thought I already knew everything about. One that is grounded in historical facts, nourished through long and extensive academic debates and finally born from the critical confrontation of my role as a first-generation German and as the daughter of North African and Arab immigrants. Without that year in Michigan, I might never have felt compelled to write these words – this very Op-Ed.

The world has changed dramatically since then. We are all watching, and our governments are watching us, too. Today's reality is more interconnected than ever. With a single click, we can watch heartwarming interactions between strangers continents apart. But with the same ease, we can also witness conflicts and atrocities unfolding live on our screens – Congo, Somalia, Ukraine, Palestine and many more. Wars and conflicts once distant and abstract are now painfully close and personal. They have never been so accessible, relatable, and immediate as today.

The ease of access to information has mobilised a generation of young people like never before. They organise and speak out, both online and offline. Yet as young voices found their digital platforms to form coalitions and respond to government policies, our governments found their own way to harness technology for surveillance. The use of digital tools to track the whereabouts, behaviour and activities of students, who actively oppose government policies has increased dramatically. But it's not stopping with students. We are now at a point where surveillance is expanded even more. The United States now want to monitor the Social Media of immigrants, claiming to safeguard religious minorities. Such measures endanger the rights of an entire generation and set a dangerous precedent for generations to come. Freedom of expression is being openly ●∴● undermined, with consequences that could alter the fabric of democracy itself.

This is the new age of surveillance… More specifically this kind of surveillance is based on what Shoshana Zuboff calls "Surveillance Capitalism". The term describes how capitalism transformed into a system that commodifies our personal data, predicting and influencing our behaviors and then monetising these to the highest bidder. This new economy erodes democratic institutions, not only allowing companies to sell our data and behavioural predictions on us to influence our decisions but offering governments the opportunity to openly monitor, surveil, and penalise citizens who disagree with their policies.

For decades, democracies have criticised authoritarian states for using surveillance to silence opposition. Now, those same democracies employ identical methods against their citizens and others. The United States actively monitors social media accounts of immigrants. In Germany, academic institutions restrict balanced discussions about Middle Eastern conflicts, and the government considers deporting dual citizens who openly criticise its foreign policy on protests.

Social media posts expressing solidarity are weaponised to detain students, revoke visas, and expel young minds from universities. Doxing websites publish personal details of protesters, endangering livelihoods and futures. Have we lost sight of who we are?

Big Tech companies paved the way for this surveillance economy. It's no coincidence these corporations were seated prominently at the inauguration of President Trump. Big Tech and governments collaborate more closely than ever before, turning behavioral predictions into powerful weapons. As responsible tech advocates, we once called for regulation to balance power. We warned of rising authoritarian leaders exploiting surveillance to their advantage. Yet, the rush for profit drowned out our calls, leaving us to witness our democratic values erode.

But while the governments watch us, we are watching them.

We see students deported for speaking up. We witness young activists penalised for daring to stand for their future. In real-time, we are watching events our grandchildren will ask us about. We bear a profound responsibility—not just for ourselves, but for future generations—to recognize the dangers unfolding.

No matter one's position on the complex conflicts and wars, all of us must acknowledge that something deeply troubling is happening. Surveillance should never become a normal tool for democracies. Our digital rights, privacy, and freedoms online are inherently connected to our liberties offline. If we fail to protect them, all our freedoms risk collapse.

We must safeguard the rights of young people who inherit the consequences of today's dangerous policies. We must ensure digital surveillance doesn't become the norm. We owe it to future generations to act now—to protect our liberties, defend democracy, and uphold human rights.

So, I ask you: When your grandchildren one day ask where you were when our freedoms were under threat, what will your answer be? ▪

Yasmin Al-Douri

Yasmin Al-Douri is a co-founder of Responsible Technology Hub, a tech ethics expert, and Senior Landecker Democracy Fellow.

Interview with

Daniel Solove



We had the pleasure of interviewing Daniel Solove, an influential privacy scholars in the U.S., on the occasion of his latest book, On Privacy and Technology, which he will present at the CPDP Culture Club. His work goes beyond academia, from his list of 50 favourite privacy books to his children's book on privacy, reflecting his commitment to making digital rights accessible and engaging across diverse audiences.

What are your plans for CPDP.ai 2025? What are you going to show or talk about?

There are two sessions that I'll be doing. First, one is based on my new book "On Privacy and Technology". It just went into print earlier this week on Tuesday. I think it has relevance for an international audience because it's about the general overview of privacy law around the world. The second one will be a session on privacy books; not just my favorite books but all the privacy books. I plan to go through my list and pick out some of the ones that have most influenced me. The list is long. However, I like the idea that I don't have to just choose one or two. I will go through all and make an overview of privacy books that I think are most notable, at least to me. I don't know the final list, but it probably will be 20, 30 maybe 40 books. It's going to be a lot.

Could you tell us about your well-known favourite book list? How did that come about and what's behind this list?

I have been keeping up with privacy books since I started in the field. For around 25 to 30 years, I've been trying to read and stay updated by tracking new books as they come out. Around 15 years ago, I began writing annual blog posts featuring notable privacy books. When I started, there were only a few. Now there are a significant number of books available, hundreds at this point. When you consider the number of privacy books available in 1999, there were very few. Currently, it's quite a lot to keep up with. However, it's exciting because there are a lot of good books out there.

Do you want to give us a hint of the few books that you think will definitely be on the list?

I'll certainly start with some notable early books, such as Alan Westin's Privacy and Freedom. I think some parts of it remain quite relevant today. Woodrow Hartzog's book Privacy's Blueprint and Danielle Citron's more recent book, The Fight for Privacy, a book or two by Anita Allen will certainly feature on my list. I'll basically review my list, focusing on books published in the 1960s, 70s, and 80s. Although there were few, there were some good ones!

One of your books especially stood out to me, which was the "Eyemonger", being a children's book, it is quite different from your other books. How was the experience of writing a children's fiction book different from your legal and academic writing?

I do a lot of reading and storytelling for my son which culminated in being steeped in children's literature. Then it suddenly hit me. I had the idea and just wrote it in an afternoon. One aspect of writing a children's book is that you can't write much. So, the writing process is much faster, which is nice. Once it was written, I worked on it with my illustrator to storyboard and we started figuring out what the visuals would be. Publishers didn't really understand the book, leading me to self-publish it and shape it exactly the way I wanted. Overall, it was a very different writing experience than the other books and I was excited to be able to do this.

What do you hope that the readers of, like the young readers of your book, will take away from this story?

I hope they'll be engaged by it. My goal was to create a fun, different, and imaginative world in which young readers could lose themselves. I wanted them to come away with something that they would remember about privacy. I hoped that they would like to be introduced to this issue and years from now they will remember something about it when they start confronting privacy issues in their lives.

As you know the conference has been already going on for 18 years now. At CPDP, we always try to bring different bubbles together and try to reach people that are not experts in laws and privacy. Translating the often dry but important topics can be quite challenging. The illustrations of the book tie well with this year's CPDP conference theme, which is "The World is Watching". Do you think we should maybe have a program for children at CPDP in the following years?

Oh, that'd be interesting! The question is what age you want to target? For instance, Eyemonger is written for kids on the younger side, like the age from 6 to 11. That's the kind of age just before children typically hop online. Once they join the online world it would require a different approach. I would certainly write a different book for a teenager versus a kid. I am thinking about the possibility of writing another children's book at some point. It might target the same age group or slightly older; just before they start getting online. However, the age at which children start engaging online seems to be getting younger over time.

Interestingly, the laws tend to view people in a weird binary way. They're either kids or then suddenly they're adults. I think it's more complicated that; a kid who's 10 years old is very different than a 13 years old, and even more different than a 17 years old. For example, parental consent just does not work the same way for 10 years old and 15 years old. I think reconsideration of the overall approach is needed.

Congratulations on your latest book which has just come out. Do you have something that you can share with the audience of CPDP?

There are a couple of features I would like to highlight. First, it was inspired when I read "On Tyranny" by Timothy Snyder. The book was written I think during the first Trump administration. It presents his ideas on authoritarianism and puts them forth in an incredibly succinct manner. It is a truly short book, about 100 pages. And I was quite struck by that. I have been thinking about synthesising my ideas and trying to make them accessible to a broader audience. So, I thought this would be a good, short, and fun project to do. So that is what got me to do the book.

One of the main questions I was trying to answer in the book is that can privacy law keep up with all the emerging technologies that we are experiencing today? We now have AI as the ascending technology; everyone is talking about. When I started writing about privacy, we did not have smartphones, there weren't social media platforms. The internet and AI were around, but it was quite different. We were just seeing the earlier manifestations of these technologies but in different shapes and forms. I ask in the book, Can the law keep up with all these changes? My answer is yes; the laws can keep up. Although laws are typically slow to react and to respond; the matter is their direction. Unfortunately, it seems the laws are missing highly crucial points and heading in the wrong direction, even the GDPR. It's partly because I believe we are

They criticise the GDPR as being a barrier to innovation. They claim that lighter regulation will increase the EU's competitiveness against the US and China. That's totally not going to be the case.



still at the stage of early attempts. It needs to evolve quite a lot, and we are far from the final word.

Another question is that why is the law the way it is, and how do we make it work better? The why part of it gets into a lot of myths that persist in our thinking about technology and law. Myths like "regulation stifles innovation". I think one of the biggest problems with the regulation is that it tries to push individual control of information; it puts way too much weight on privacy rights and individual responsibility. So, what must be done? In the simplest terms the creators and users of technology should be held accountable, both before and after. So that they can't be putting out dangerous products. It must be ensured that what they're putting out is safe and not damaging to privacy, and not harmful to people. If they put out something dangerous, there must be strong, dissuasive enforcement. I think not just in the US but also in the EU, the enforcement is not enough. Even the GDPR's big fines fail to change the ultimate equation. The law often grants big tech companies and technology users a free pass. The profits are astronomically high. Why would a company not just do what they want to do? Companies scrape the Internet or act irresponsibly, only to later say "oops, sorry, we didn't know" when regulators intervene. They'll always come up with something after the harm has been done and the penalty is never going to be enough to prevent them in the first place. That is simply not enforcement.

So, the book is focused on how we build laws that adhere to this basic principle and hold them accountable. Pre-emptive strong enforcement for companies works, and it worked for centuries for everything else. But the law finds every way to treat technology differently; to give it worship or to fear it. Technology just gets treated in a different way than almost everything else, a kind of techno-exceptionalism. Let's say they have a bug in their software; it's not their fault. They cannot be held accountable.

Somehow, policymakers get very daunted when they see technologies. They are not experts, so they don't want to stand in the way of innovation. This is how myths shape the law. Think about car safety, a seat belt is just as much innovation as a gas pedal in a car. The car manufacturers had to be forced to innovate for safety. They didn't do it on their own. Currently, the law often does not reward these sorts of innovations. It basically encourages companies to move fast and break things, and this is fostering irresponsible innovation. Why isn't privacy an innovation? This is basically the gist of the book.

Do you think it's true that the GDPR is not good enough? If so, in what way do you think it should change to be improved?

I think that the GDPR is not strong enough. It is formalistic in such a way that it loses sight of the principles that it's trying to protect. It relies too much on individual rights and responsibilities. The whole approach to consent and cookie banners loses the bigger picture. But the attacks on the GDPR often come from the other direction. They criticise the GDPR as being a barrier to innovation. They claim that the lighter regulation will increase the competitiveness of EU against the US and China. That's totally not going to be the case. A weakened GDPR would only benefit the pockets of US companies or further advance China's surveillance state agenda.

Similar arguments were trotted out after the September 11th attacks in 2001, this case through security vs privacy myth. Most government measures introduced to protect us didn't really provide much protection. Instead, they fostered a surveillance state without providing any benefits but rather a rollback in the law and accountability.

The truth is you can effectively have concrete accountability and much better protections that would do both. I wrote a whole book about this 15 years ago. The same thing is going on here. Tech companies want to do whatever they want, and they don't want to be held accountable. This is where the innovation vs regulation myth comes in. The reason why the EU doesn't have the same kind of tech industry as the US has nothing to do with regulation. It's just the money; the venture money is not there. So, it must be funded. Also, the companies in China do exist because the Chinese Government funds them.

In the US, the tech industry arose in California. If the innovation vs regulation myth was true, the tech industry wouldn't take place there. California has the strictest privacy regulations in the US. So why California? Because that's where all the talent was. It had nothing to do with regulation.

Currently, the Trump administration is basically killing the goose that laid the golden egg by destroying pretty much everything that nurtured the US tech industry. It's a great chance for Europe to step in. But certainly not with the recipe of the Trump administration, which is to jeopardize universities, research, and create a miserable environment, which won't bring in the kind of talent is needed to do this.

They are going to tear down the tech industry by favoring the oligopoly of big companies over newer competitors. They just want to be the ones. If they succeed in annihilating the infrastructure in the US; the technological research, universities, culture, all that is going to be wrecked. So, there's a very high chance that the U.S. will not be the place where the technology is. If Europe sees the right recipe and learns the right lessons, it could be Europe. Europe could be the next one, as the US is basically heading toward self-destruction.

What do you hope for our conference and what are you looking forward to?

I've heard about it for many years, and I have long wanted to attend, but I've never been to this conference. The timing has always been tricky for me, as I organise two conferences around this period. The timing works out perfectly this year as it falls between those two conferences. It's also an important time to address these critical issues.

This is the moment where the EU is going to be tested by these challenges to regulation. The question is whether the EU will backslide or stand firm in its values? Additionally, the GDPR does need a new approach to privacy laws as a whole. The EU needs to take a deep look at their privacy law and examine why it is not working and explore strategies to improve its effectiveness. ▪

This is the moment where the EU is going to be tested by these challenges to regulation. The question is whether the EU will backslide or stand firm in its values?

CNIL POLICY BRIEF – MARCH 2025

What are the economic benefits of a company's DPO?

OPINION PIECE

The French data protection authority CNIL studied the economic benefits of having a Data Protection Officer (DPO) for a company and the conditions under which this return can be harnessed. Statistical evidence illustrates the profitability of the DPO, particularly if the company has an active approach to GDPR compliance.

At the request of the French Ministry of Labor, the Association pour la Formation Professionnelle des Adultes (AFPA) conducted the fourth edition of its statistical survey on Data Protection Officers (DPOs) in January 2024. The survey is statistically representative, with 3,625 respondents and allows to study the economic benefits of having a DPO in the private sector, notwithstanding the mandatory nature of this function in some cases.

CNIL also led qualitative interviews with 10 DPOs recommended by the AFCDP, a French representative DPO organization. Those interviews help confirm the interpretation of the survey results.

The economic benefits of DPOs

From the survey, we can distinguish different types of economic benefits to the presence of a DPO: fine avoidance, reduction of cybersecurity risks, improvement of the company's public image, and as a lever to win tenders. But those benefits are not perceived by all companies which hire DPOs.

The benefit of improving the company's public image

In companies that develop a brand image incompatible with non-compliance to GDPR, DPOs have an essential role to preserve the enterprise's public image.

During interviews, many DPOs have noted that public fines have a negative impact on sales and also on financial ratings: compliance can therefore have a positive impact on a company's production cycle and financing capacity.

The benefit of compliance as a lever to win public tenders

According to DPOs, GDPR compliance also has a role to help the company win public tenders. In some structures, the DPO actively participates to the mobilisation of GDPR compliance as a way to increase trust, optimizing the probability of winning tenders.

For example, one DPO explained that following a strategy of public communication on compliance, the probability of winning tenders increased by 50%.

Interviews also revealed that some DPOs envisioned their roles above insuring that their employer is compliant. They also actively participated to the valorisation of compliance, for example, by including GDPR compliance to the CSR strategy of the company.

The benefit to fine avoidance

In 2024, CNIL issued 87 fines for a total of 55 million €: as such, there is a real advantage to avoiding them. Statistical regressions carried out on the study data show that the benefit of avoiding sanctions, as assessed by the DPO, depends on the size of the company and its business model.

The benefit of avoiding fines increases with company size as bigger structures are more likely, all other things equal, to face fines or to be the subject of a complaint than smaller ones.

Companies whose business model depends in great part on data also perceive an important benefit to avoiding fines due to the greater reputational risk for these structures. If the fine is made public, the monetary cost is less important than the negative impact on the reputation of the company for its clients, partners, etc, especially for companies offering innovative, potentially intrusive solutions (voice assistants, etc.).

The benefit of avoiding data breaches

Cybercrime represents important costs for companies. For example, the IBM 2024 cost of a data breach report showed that the average cost of a data breach is 5 million USD, up 10% on 2023.

Compliance implies implementing appropriate cybersecurity measures (Art 32 GPDR), so the DPO has an important role to prevent data breaches.

This benefit follows the same pattern as sanctions in terms of reputational impact. A company whose business model relies partly or entirely on data is at risk of reputational damage in the event of a large-scale data breach.

This benefit can be achieved by any DPO with enough time to implement appropriate security measures for the processing of personal data. For example, one DPO reported that after introducing phishing awareness training, the click rate on suspicious links within the organization dropped from 21% to 5%.

The benefit of streamlined data management

The principles of the GDPR (Article 5) push companies to be frugal in the collection of personal data, which necessarily leads to operational savings. During our interviews, a DPO of a company with sales of 150 million € explained that GDPR compliance has saved 400,000 euros in server costs.

This streamlining of data also brings benefits in terms of cybersecurity. The role of the DPO involves precise mapping of databases: knowing where they are stored, who has access to them and where copies are located. This reduces the risk of leaks and attacks by limiting potential vulnerabilities. Less stored data also means fewer entry points for cybercriminals, and therefore a reduced "attack surface".

Better knowledge of data also facilitates its exploitation by centralising information and avoiding duplication or data silos. Teams can then access relevant data more easily, improving the efficiency of internal processes and decision-making.

The impact of the business model on the DPO

There are differences between the working conditions of DPOs, depending on the structure's investment in compliance. A small minority of the DPOs have their own budget, a few of them are also less linked with the CSR team.

The DPO function can be considered as an investment: the companies granting more resources to DPOs are also those who derive the most benefit from them. Among the latter, we find structures that fear DPA fines and companies with a business model in which data plays an important role.

There is a return on investment in the sense that DPOs who have more time to dedicate to their function are in a better position to ensure the company's compliance, which helps reduce the likelihood of incurring a fine.

As well as affecting the resources available, investment in compliance also affects the way in which DPOs experience their role. For example, DPOs who find it difficult to carry out their duties, are little consulted, and receive little training tend to be less satisfied with their job.

Conclusion: Compliance as an Asset

Compliance with the GDPR is mandatory and entails undeniable compliance costs. However, a company can make its compliance profitable by leveraging it as a valuable asset.

Article 37 GDPR outlines specific cases where companies must appoint a DPO, which leads some organizations to see the DPO as a constraint (89% of DPOs surveyed report that their organization perceives the role as a burden). However, there are economic benefits to GDPR compliance that can be harnessed when compliance is treated as part of the business model. The investment made in compliance can offer financial returns, like an asset.

With such a strategy, the DPO becomes a key figure in making compliance a profitable and valuable investment for the company. To unlock the economic benefits of this role, there must be a clear awareness of these advantages among decision makers, as well as a well-defined position and roadmap for the DPO within the organisation. ▪

Aymeric Pontvianne
from La Commission nationale de l'informatique et des libertés (France)



Interview with

Safa Ghnaim

Safa Ghnaim is Tactical Tech's Associate Programme Director and Project Lead for the Data Detox Kit project. She also leads the Data Detox Bar project at Tactical Tech, which you can visit on the 2nd floor of Maison de la Poste.

The theme of this year's CPDP.ai conference is "The World is Watching". What does this theme entice in you in the context of privacy and data protection?

That is an interesting provocation, especially since technology is always advancing. AI was not just produced yesterday, it's been this ongoing trajectory of evolving systems, like algorithms that then eventually evolved into these things that can produce images with the click of a button. *The world is watching* and waiting, to see how it's going to evolve.

Personally, I don't like how the onus is often placed on consumers to act differently, to consume differently. Of course, we should be more aware of the information we consume and share, how we spend our money, and how that impacts society and the environment — but these are systemic issues. They are rooted in trillion-euro business models. What people I know are looking at is; *When will technology be taken more seriously, properly regulated, and when will we (people and the environment) be protected better against the harms that are coming out of them?*

In the past, people would think, oh, well, e-waste is being shipped somewhere else, mining of minerals is far away… but now, gig workers, factory workers, and delivery drivers are really struggling under these conditions, right in our own communities. Although we're taking steps to become more mindful consumers, and to better understand these systems, we would also benefit from proper regulations or protections that are beyond what we can produce ourselves as individuals.

The *Data Detox Bar* will be present at CPDP this year for people to visit. Can you tell us more about the concept behind the *Data Detox Bar* and what inspired its creation?

It all started with *The Glass Room,* which was this huge exhibits with actual glass windows and where everything was white and shiny and illuminated in Berlin, London, New York and San Francisco, and now available as a pop-up version. It examines how technology is impacting societies and particular themes around data collection privacy, online safety, online influence and many more topics that were being covered in these Glass Rooms. Visitors would ask us on their way out: *what can I do about this?* They were looking for tangible actions and that's how the Data Detox Kit was born.

The *Data Detox Bar* is a central meeting point, in *The Glass Room* and in other exhibitions, where people can come, sit down, take a rest, and talk to somebody, maybe ask questions or get some thoughts off their minds. Because technology is a lot to make sense of sometimes. In the past few years, we've further developed the bar to be modular, allowing it to travel beyond *The Glass Room* to conferences like CPDP, to be that space with concrete, tangible tips.

What are some of the most common data privacy concerns people bring up when they visit?

People bring up concerns that I can relate to, some I've worked through myself, others I'm still figuring out. A common fear is that it is out of their hands, that there's nothing they can do. While that concern is valid, it is not impossible. Even if there may not be a perfect way of cleansing your data or reducing your footprint, there are still helpful steps one can take.

I have heard people say *"I don't have anything to hide"* or *"I can figure out misinformation"* this led to us having talks on maybe *you* can but what about your neighbor, your child or your grandparents?

I've gotten a lot of questions from people about passwords, too. It's interesting to hear different perspectives, for example from hackers and developers as well as from people who have less technical skills.

How has AI influenced the *Data Detox Bar*?

Before AI and the ChatGPT boom, our materials focused on reducing data traces, browser history, screen time, media literacy, and passwords, and these *are* still relevant today. Our new resources address how AI amplifies existing issues like scams, harassment, and bias by deepening them, making them faster, more believable and easier to spread.

When discussing AI, we focus a lot on demystification, helping people understand what AI *actually is*, instead of just step-by-step actions like "go to your settings and change this". We vaguely break down common AI tools like large language models (LLMs), synthetic image generation, and offer a lot of contextualisation.

The *Data Detox Bar* has been present in several countries, have you noticed any differences in the privacy and digital rights concerns raised by visitors based on their region?

Yes, there are definitely a lot of differences in attitudes around privacy in general. Even in places where privacy is highly valued, and even when privacy at its core is really important in certain communities, the way they look at technology can sometimes feel very distant. For example, when discussing the Data Detox Kit in more conservative places, I have found that while privacy is culturally significant, many people don't mind using the same password everywhere or relying on WhatsApp for all their communication. But once we get into these open conversations about, *where does your data go? Who has access to it?* people become very reflective and open to change.



We're taking steps to become more mindful consumers, and to better understand these systems, we would also benefit from proper regulations or protections that are beyond what we can produce ourselves as individuals.

Even in places where privacy is highly valued, many people don't mind using the same password everywhere or relying on WhatsApp for all their communication. But once we get into open conversations about where their data goes, people become very reflective and open to change.

When I was at *The Glass Room* in San Francisco, right in the heart of Silicon Valley, we saw a mix of perspectives. Some visitors felt privacy wasn't that important to them or believed they got it under control, "*I have one really strong password; no one will ever guess it.*" At the same time, we had people visit who were working at these tech companies and I remember there was one person in particular who was a developer and said they felt guilty and frustrated because they were the one who creates these tools and didn't like how they're being used. It was interesting to see also that kind of sentiment was coming from people even when they're part of these companies. At the end of the day, they are not usually the decision makers, they're given directives and tasks, and they don't always know how these tools are going to be implemented.

How does the Data Detox Bar relate to other Tactical Tech projects like The Glass Room or the Digital Enquirer Kit?

I might be biased since I co-wrote it, but the *Digital Enquirer Kit* is one of my favorite projects, and I wish for it to get more attention. It's an open, free e-learning designed to teach investigation skills. We wrote modules 1, 2, 3, and 4, and there are two or three other modules written by other orgs. The modules that Tactical Tech wrote are about conducting research and working in teams to do that research. We relied on expert resources from ***Exposing the Invisible,*** another Tactical Tech project created by experts. My core team for Digital Enquirer Kit, which included three digital security experts from different regions, worked to make these thorough, detailed resources from *Exposing the Invisible* more accessible.

The e-learnings are easy to follow, for people who are in a hurry.

This connects directly to the *Data Detox Bar* and *Data Detox Kit* because all of these projects take complex technical topics and make them very easy for anyone to follow and reflect upon. The Digital Enquirer Kit has been used in libraries, classrooms, and community centers and to train very intentionally students which has been really motivating, and I hope more people can check it out.

Can you tell us a bit about Tactical Tech and how the organisation has evolved over the years?

Tactical Tech was founded in 2003. While it has evolved, some parts have stayed the same, such as the focus on privacy and safety online and how technology impacts societies.

In the past, there were more regionally focused projects at Tactical Tech. Today it's more international and we support partners to adapt our resources to their specific contexts.

For me personally, working at Tactical Tech for nearly seven years has meant having the flexibility to follow different curiosities. Of course, they have to fit within our mandate and grant requirements. But it is fun for someone like me who changes and evolves my interests and is able to move with those and create meaningful projects and outputs.

Tactical Tech has since its foundation promoted the use of open source software. How have perceptions around open source software developed among the people that you work with? Has it become more challenging to promote software like Thunderbird and LibreOffice?

We use open source tools in our day-to-day work as a requirement. Some of these tools are very intuitive whereas other tools maybe require a little bit of practice or setting up. Sometimes there is a bit of friction or it requires more time, so that sometimes people feel like they need to be trained in it to use it really well.

For all tools, it is important to keep a constant watch on how their business models and practices are evolving. For example, the Terms of Use of Firefox, changed, and so we are reassessing how it fits within our scope. This isn't unique – regularly, we have to go back to reassess our tools to see if there have been any changes. It is not easy for them to function in their businesses when they are competing against giants like Google and Microsoft.

Yes, it seems to have been in the making for a while. The competition has been tough on them. I remember when implementing some digital security measures, I read a report that said that open source solutions were less secure for cloud hosting than what Microsoft offered. This challenge that civil society has when working with open source tools is familiar and requires support but the trade-offs are difficult to estimate.

The same trade-off can be said for some of our audiences and collaborators as well. We each may have different threat models and risks. When collaborating with people in certain contexts, for example, using Google products like everyone else might actually be beneficial for them, compared to using VPNs, which could possibly raise suspicion. There is no one-size-fits-all solution and it should always be assessed and considered on a case-by-case basis.

As the societal role of digital technologies continues to increase, and while governments are diverging in their responses to the challenges that digital technologies pose, how do you see the role of civil society evolving?

I'm definitely still trying to figure it out myself. I recognise that we're in a special, unprecedented time where it's difficult for civil society and NGOs in general to do their work due to funding struggles, political consequences and risks. Looking at what's happening around us, it sometimes feels like we're living in a fictional novel. This would be funny if it wasn't so scary.

We are all interconnected: funding cuts in the U.S. affect civil society there, and the rest of the world are absolutely affected by this as well. I have hope that things will eventually get better, but I'm not sure what the road to "better" will look like. Right now it seems very difficult for everybody.

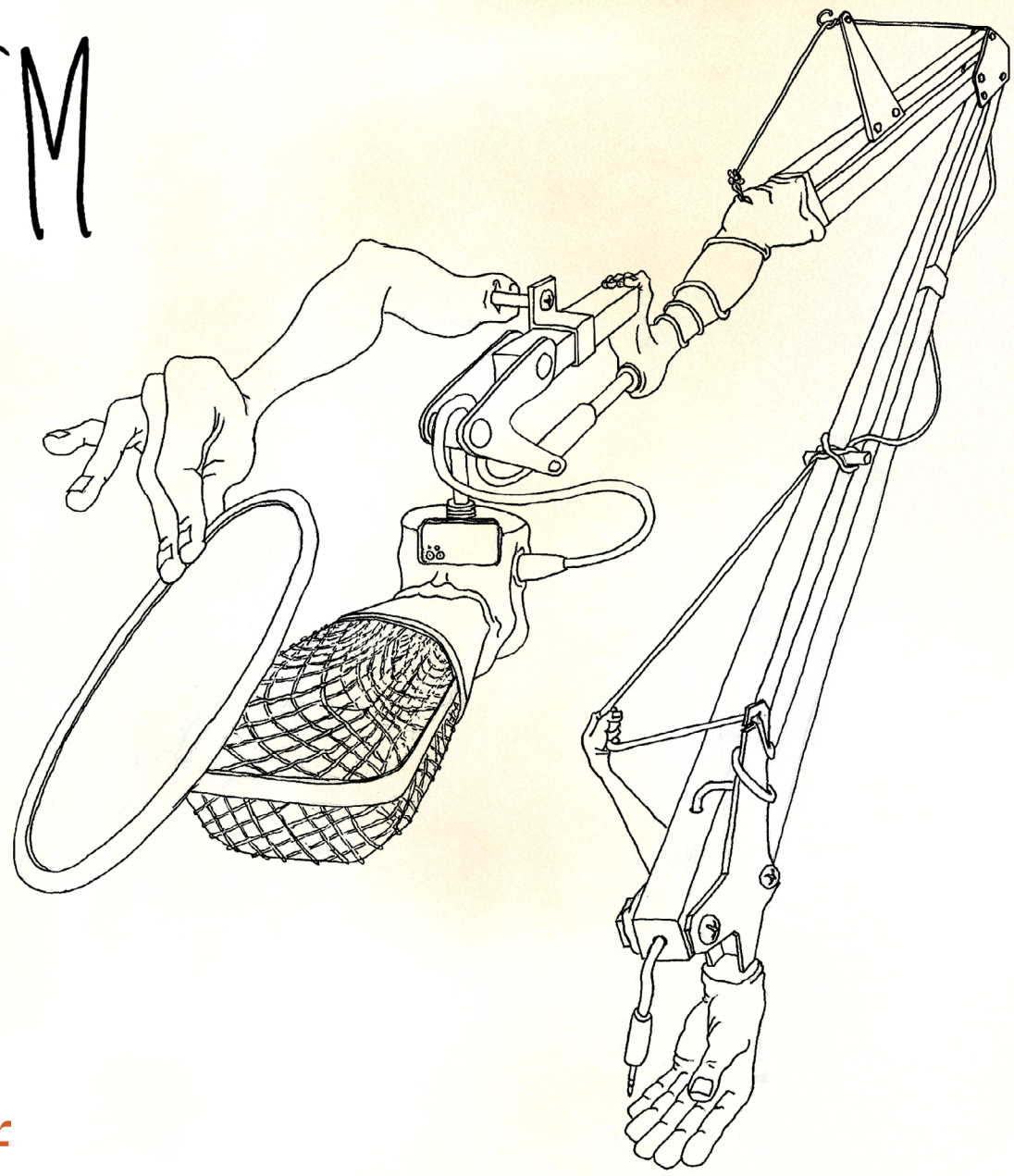
I am really grateful for having such an amazing network personally and professionally in our field. We might feel like we must navigate these struggles alone, but alliances, even if they're patchwork or unofficial, just having this kind of support, is very helpful. If we stick together and help to raise each other up and collaborate it can only make us stronger. ▪



Data Detox Bar | Photo by Tactical Tech

CPDP.ai • Live Radio • 3 Days • On-site at CPDP.ai • Live Radio • 3 Days • On-site

AVATAR.FM



May 21–23 2025
Brussels

For CPDP.ai 2025, Privacy Salon and community radio station dublab are teaming up again for Avatar.fm, a temporary radio broadcasting live from CPDP.ai on three consecutive days.

Location:
in front of the Grande Halle

Check out the programme at
www.cpdpconferences.org

Tune in live at dublab.de

Giving a voice to the young and new generation of privacy, data protection, AI, and computer scientist heads, Avatar.fm amplifies stories and testimonials of students, junior researchers, artists and activists in the form of Console Talks & Data Dialogues. These can evolve into longer debates with the participation of a live audience.

Feel free to drop by and engage in conversations about the datafied world and AI related subjects, interwoven with DJ-sets by numerous dublab favourites live from iconic Brussels venue Gare Maritime.

DUB LAB × Privacy Salon

n-site at CPDP.ai • Live Radio • 3 Days • On-site at CPDP.ai • Live Radio • 3 Days


© Anna van Kooij

Interview with

Bart van der Sloot

We celebrate a birthday: the tenth anniversary of the EDPL's Young Scholar Award. Hence, we talked with one of its founders: Bart van der Sloot, who specialises in questions revolving around law and technology, Artificial Intelligence and Human Rights. He is associate professor at the Tilburg Institute for Law, Technology, and Society, Tilburg University, and is the Editor in Chief of the European Data Protection Law Review.

Could you tell us about how the idea for the journal of European Data Protection Law Review (EDPL) originated and how it turned into a reality?

We were already discussing the idea of founding such a journal because we recognized the need for a European focused journal on data protection and privacy law. Although the community was already big and growing, including regulators, academics, and practitioners, we felt the absence of a central platform. Our goal was to bundle those approaches by providing a platform for diverse interest groups and players.

The journal has a section dedicated to academics to put forth new thoughts and scientific insights. We also have a report section that addresses regulatory issues at a national level; a section dedicated to cases by both the Court of Justice of the European Union and by the Human Rights Court; a Book Review section; and a section for interesting topics and opinions where more vocal pieces contribute to debates.

We aim to provide a platform where everyone can gain valuable insights on data protection and privacy law from a multidimensional perspective. So, the idea was already there, and with the GDPR being in the works, adopted yet in effect, we knew it was the right time to act. Then, we decided to go for it. This is how it began.

How has the journal changed over the last 10 years, and where do you see it going in the next 10 years?

When the journal first started, we focused on straightforward legal analysis of the GDPR. We were trying to figure out what does it involve, what does it practically mean, and what kind of effect it will have. There were many court cases concerning the interpretation and conflicts between different jurisdictions. In a way, we were entering uncharted territory. That said, the focus gravitated towards a more analytical direction over time. We started questioning the type of regulatory approaches and addressing their effectiveness. Also, questions like "How does this compare to the US or Chinese approach emerged? This transition was already in motion. I am confident it will continue over the next decade.

Currently, data protection is becoming a part of a broader regulatory ecosystem, reflected in new instruments like DSA, DMA, AI Act, Data Act, and Data Governance Act. The GDPR still remains the foundational framework, what we often refer to as the "mother ship" on which these newer regulations are built. Currently, we focus on exploring how the GDPR can support other areas, such as human rights law, and increasingly competition law. Data protection, especially in the light of the AI Regulation, plays a crucial role in shaping decisions; a trend I believe will continue in the coming years.

While the future is uncertain, it seems to me that it will lead to a more global political vision for the EU's regulatory strategy. For example, if we aim to build an AI sector, how should we approach it? Should we nuance certain rules? Or should we keep our principles and human rights laws in place that prohibits all American and Chinese AI and LLMs that do not align with these principles? Since they don't conform with these principles, can we say: "OK, all non-European systems are simply banned in Europe." That way, all our data stays within Europe and we can use those data to build a European AI sector based on our own values and interest. This broader political regulatory debate is also hanging over the more nitty-gritty legal discussions that remain in question.

There is a strong relationship between CPDP and EDPL's Young Scholar Award. What are some of the strongest memories that you have when it comes to winners? And do you think participants have gained through this collaboration with CPDP? How important has CPDP been as a platform and a meeting point for so many worlds, influencing some of the participants, or the award itself, or even you?

First, the idea behind the Young Scholars award is to provide a platform, a springboard for the next generation of academics, practitioners, regulators, and many others in the field. Our goal is to support and push them. That's where I see CPDP's venue is of huge value. This is a place where everyone in the community comes together. It's a great opportunity to introduce those young scholars to this network, to make them seen by the CPDP community, to get them recognition. That's why we always wanted to ensure that the awards are given at CPDP and not anywhere else.

We aim to provide a platform where everyone can gain valuable insights on data protection and privacy law from a multidimensional perspective.

I am incredibly proud to see that many of those who won the award or were in the top three have gone on to become excellent academics, practitioners, and regulators and they kept staying active in the community.

One memory that stands out is of a PhD student who was on the verge of quitting, feeling completely stuck. She reached out, was ready to give up. We encouraged her to wait for a few weeks. Soon after, her paper was selected for presentation at CPDP –and she won

the award! This provided the boost and the confidence to continue. I feel this is something we all can relate to as academics, but especially PhD candidates who often work in isolation and wonder "What am I doing with my life?", "Does my work matter?" Receiving that recognition is more encouraging than the prize itself. We also record short clips with the winners and the other participants. They often get many responses from regulators and other academics saying things like "This is really interesting! Can you also come and speak at our conference?" This recognition and networks provided by CPDP is often a turning point for many. This is something that quite often happens and this is one of the things that I am most proud of.

What have been the hardest parts of being the editor in chief of the journal, and is there anything of the last 10 years you would change looking back now?

We deliberately chose to focus on Europe, and this is our strength, but also is a limitation. As a journal for the European Community, it does connect all these different groups and stakeholders within EU. However, it misses substantive discussions and understanding between Europeans, Americans, and the East Asian community; those three regions operate independently.

It's rare for scholars from one region to contribute and write for another. This is due to the differences between mindsets, argumentation styles, and writing styles. And also, because we live in such a polarized world where different groups don't really understand each other and are even alienated and hostile towards one another.

We often think about how we can bridge that gap in a real, substantive way at least for our community as a first step. In every edition or on specific themes we address the question of whether we can keep our European ideals while incorporating Asian and American perspectives.

What do you think the most important subjects for the future will be?

I think the most important question is: Are these rules adequate in achieving their legislative goal? It is also important to recognize that data protection laws date back to the 1970s. Since then, the core hasn't changed much; the underlying values still remain highly relevant—perhaps more than ever. However, the way these rules were written may not always be the most effective one in achieving their goals. Instead of simply checking if a new technology aligns with the legislative framework, we should be focusing on the underlying values. Too often, compliance is reduced to a checkbox exercise which adds little meaningful analysis. I think we should go 👀 back to the underlying values. Also, because there has always been a sentiment —it's something that's reappearing, especially now with AI— that these rules are blocking progress. It's not enough to just say, "It's the rule, and you're not conforming with it". We must be explaining why it matters. For example, we now see that Elon Musk have access to all governmental data and using it to threaten senators who oppose his political line. We must understand that this is why privacy actually matters! This is the most vital interest we aim to protect—ensuring that governments stay neutral and won't abuse their power.

I think we should be asking first whether something is a problem and why, before considering how the law applies. That consideration should always come first—rather than simply declaring that the rules and regulations are blocking progress or simply sidestepping them.

The CPDP theme evolves alongside global events, constantly adapting. This year's theme, "The World Is Watching", feels especially holistic. How do you interpret it in the context of data protection law? And how do you see it resonating with the EDPL Young Scholar Award and its contributors—the very people shaping global perspectives on privacy and data protection?

I see this as a time of spectacle. Countless events unfold daily while we watch passively —but I feel we need to turn it around. "The world is watching us: what are we doing? How will we tackle these emerging challenges?" As Europeans, we must adopt a more strategic global mindset. Change is always slow in the EU, but it gives a strategic stability in comparison to more radical approaches elsewhere.

Young scholars are observers of today's challenges, and many feel disempowered or anxious. I always remind them: "The world is watching you!"—not to burden them, but to highlight their power to drive for a change. If anyone can, it's their generation. That's why I want to provide them with a platform, and I'm very happy that CPDP as well facilitates it. I often have disagreement with my PhD students, but it's a good sign. Their ideas must be bold, radical, and new and antagonise me and my peers. What I hope for is that this generation embraces their responsibilities, recognises what's broken, and says, "We'll do things differently".

Also, for the data protection community, I would encourage them to fully revise or reconceptualise the GDPR framework. Although it's logical, it needs revision to meet today's challenges.

For me, every day is a new beginning. We must constantly rethink what we're doing—even when it still makes sense.

Yeah, the world will be watching that statement.

Exactly! Also, they must ensure that the world is watching them. They have to stand up and say, "Look, enough of this nonsense. We are the next generation, and we will tell you how it's going to happen".

As you are celebrating the 10 years of EDPL journal, what message do you hope to leave for both experts and the next generation of data protection?

For me, every day is a new beginning. We must constantly rethink what we're doing—even when it still makes sense. We should always step back and ask: "What does this mean for our society? How do we want to live? And how can law help achieve that?"

You mentioned that CPDP always has a new theme which resonates with the world. That's why CPDP stays relevant—you ride the tide but also pause to ask: "This is happening. What does it fundamentally mean"? I hope we can do the same with EDPL Young Scholars.

For the 10 years celebration. Is there a cake? And did you order cake? And who's going to blow the candles?

There should definitely be a cake, and if anyone should blow out the candles, it's Nelly Sativa, our managing editor. She's the behind-the-scenes force that makes everything work. While I am the spokesperson, Nelly and her team are the backbone. So, I'll buy a cake, put candles on it, and ask her to blow them out!

Excellent. I want to be present.

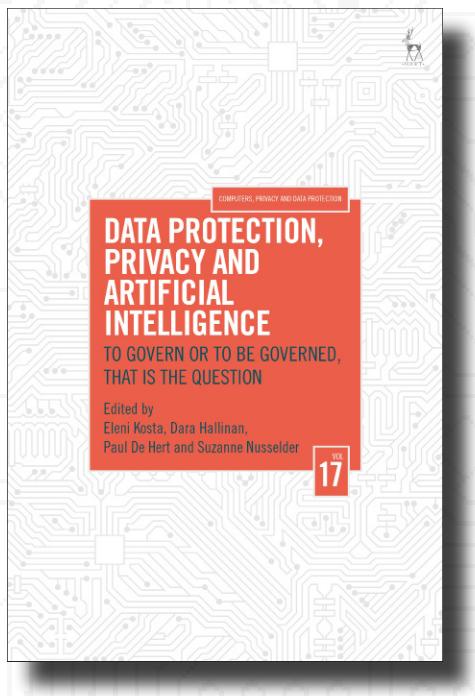
Thank you. That will be wonderful. ▪

VOLUME 17

Data Protection, Privacy and Artificial Intelligence

To Govern or To Be Governed, That Is the Question

Edited by Eleni Kosta, Dara Hallinan, Paul De Hert and Suzanne Nusselder



May 2025 | 328pp | Hbk | 9781509984015 | RRP: £55 / €75

Copies will be available for purchase from the conference bookshop, or you can order on-line before **23rd June 2025** at **45% discount**. For EU customers: order the hardback via **www.groenewaterman.be** using the discount code **CPDP2025**. For customers in the rest of the world and for ebook orders: go to **www.bloomsbury.com/cpdp** and use the code **CPDP2025**.

This book examines the discourse and developments surrounding privacy and data protection in the digital realm, featuring papers and discussions from the 2024 CPDP.ai international conference.

The question of governance—whether to lead or be led—has never been more relevant. Thus, the book not only addresses privacy and data protection, but also highlights issues related to the governance of artificial intelligence and the regulatory changes introduced by the EU AI Act.

The book features comprehensive discussions on the adequacy and effectiveness of the governance mechanisms established by the EU AI Act, particularly emphasising standardisation, co-regulation, and human oversight, while also identifying existing gaps in protection. Additionally, it pays special attention to the risks to fundamental rights associated with AI usage by law enforcement agencies, examining whether the current legal framework sufficiently safeguards against these risks. Finally, the book provides an in-depth exploration of deepnude and deepfake technology that generates nude images, as well as the role of AI in the EU's migration management systems.

The chapters in this book provide readers with an opportunity to explore the challenges and developments related to privacy, data protection, and artificial intelligence. By presenting academic insights alongside contributions from practitioners, civil society, and the European Data Protection Supervisor, this interdisciplinary volume encapsulates the essence of the CPDP.ai 2024 conference.

Eleni Kosta *is Professor of Technology Law and Human Rights at Tilburg University, the Netherlands.*
Dara Hallinan *is a Legal Academic at FIZ Karlsruhe, Germany.*
Paul De Hert *is Professor of Law at Vrije Universiteit Brussel, Belgium.*
Suzanne Nusselder *is a PhD Researcher at Tilburg University's Institute for Law, Technology and Society (TILT), the Netherlands.*



Are you interested in contributing a chapter to **Volume 18**? **Roberta Bassi** is available to answer your questions at the conference or by email at **roberta@hartpub.co.uk**

Visit **www.bloomsbury.com/cpdp** for more info.

HART



Interview with Frances Haugen

CPDP has encountered many critical voices in its eighteen years of existence. Not everyone has made it to our stages (yet). When we witnessed a fiery keynote by Haugen at MozFest in Amsterdam a while ago, we knew that some day, we had to continue the conversation for a short interview in the CPDP.ai magazine.

In an age of interconnectedness where privacy is heavily intertwined with other individuals, how do you interpret this year's CPDP theme "The world is watching"?

The rights that we demand and negotiate with our governments, and the willingness of our governments to actually fight to enforce those rights is so important.

We've known for a long time that we "bleed" information-very intimate personal information-via who we associate with. You can analyze someone's network on a social platform like Facebook or wherever they choose to spend their time. These platforms learn a lot about a person by inference, just because we hang out with people who are similar to ourselves.

Even if you are relatively private online, just by participating in these spaces at all, you end up spreading a lot of very personal information-for example, your sexual orientation. And as a result, there should be guardrails placed on these companies-rules around what they're allowed to do with our data, how they can target us, what kind of information is given to us, and what kinds of controls we have over how that information is delivered to us.

As you can imagine, one response to having better data privacy laws isn't just about what can be used for advertising or what is shared outside the company. It's also about questions like: Should you be allowed to reset your algorithm? Should you have an easy right to reset?

And what's nice about this concept is, I've been advocating it for a couple of years-and for the first time, Instagram integrated the ability to reset your algorithm just a few months ago. They don't make it very easy, but it is there. Because in a world where they can accumulate information on you, you can end up in a situation where your view of reality becomes very, very tailored. All that information they've collected is used to influence what you're allowed to consume. So having the right to dig yourself out of that algorithm should be something everyone is entitled to on every platform.

With increasing transatlantic pressure on EU regulations, how can the Digital Services Act and General Data Protection Regulation remain effective and significant going forward to protect digital rights and personal data?

We are living in a very exceptional age. Watching how things are playing out in the United States really reinforces why it's so important that Europe channels Charles de Gaulle and says: We can't trust that America will remain constant. Like all places it's going through change.

Part of that discussion has been about shared defenses. Should Europe have its own infrastructure for various things? Because if the US elects people who don't honor treaties or don't believe in mutual defense, that leaves Europe in a very awkward place. And I think there is a similar conversation to be had around digital infrastructure.

What does this mean? There's a really important conversation to be had around what Europe should be doing to invest in their own digital infrastructure because we act as if it's impossible to have our own social spaces. But imagine if we went into schools and you proactively took measures to learn about how these platforms work. In the US, we have programs implementing community-based digital detoxes. November is our mental health month. Nonprofits go into schools: in September, they educate the community; in October, they talk about the perils of online addiction, how algorithms influence the US, rabbit holes, and privacy rights; and then in November, collectively, the whole community takes a break together to remind themselves that they actually like spending time in person with each other.

These are decisions we don't get to make individually-we have to make them collectively. You may want to spend more time in person with your friends, but if they don't make that decision at the same time, it's not really a choice for you, right?

Now imagine a world where Europe came in and said, "We're going to go and talk to kids. We're going to find out what their needs are. What would an ideal platform for them be? What would public infrastructure be like? What would it look like if we designed for linguistic equity upfront?"

Back in 2004, the reason Facebook beat Friendster-then the biggest social network in the world-was because they figured out how to run the infrastructure. It sounds like it shouldn't be complicated, but it is complicated math. Things like who are the friends of your friends was a question that made computers melt in 2004. Today, very simple computers can do those calculations for very large social network systems.

One of the things that I really want to emphasize, especially for young people in Europe: a new social platform begins with just two users.

So, what would it take for Europe to have our own version of Instagram? Because we can't count on America to not be digital colonials. And that's what this conversation needs to be rooted in–not just on whether we can rely on America to honor our laws, but whether we can we rely on America to acknowledge the exploitation or the negligence.

There are more speakers of French Canadian than speakers of Norwegian and Danish, yet very clearly, there's no protection for children against self-harm content or against content that encourages the taking of one's own life, both which they can freely access. There are networks that continue to distribute this content despite the number of years that they've asked for something to happen, and the only explanation I can come to is that someone inside these social media platforms decided that Norwegian wasn't important enough a language to justify providing basic safety systems for children.

This is the reason why I keep planting this idea: What if Europe decided we cannot rely on America for our digital public spaces? These things grow. If you go to Silicon Valley, the tech people aren't using Meta products–they use spaces like Signal, an open source, end-to-end encrypted, peer-to-peer messaging app.

I would really love to see people channel the anger and the despair they feel right now and say, well, what if we did dream bigger? What would a European alternative to all of this look like? I think it's there. I think it will happen. And honestly, I don't think it'll be that hard.

People say dreams like that are impossible, but remember–Facebook originally spread from college to college. If you go to middle schools, high schools, and colleges, we can build a community. Make it a political statement. Make it a statement of self-care. Make a statement of caring for each other. That's how you build inertia, because wherever the young people go, the older people eventually follow.

Since most social media platforms work with black boxed algorithms where even the employees don't necessarily understand how they work, what would you say are some practical steps to ensure algorithmic transparency going forward?

Employees are always learning how the algorithm works in real time. Every small tweak causes first-order, second-order, and third-order effects–many of which are often almost impossible to intuit or predict.

Physicists are some of the most effective people at studying algorithms that influence and shape our realities, because they're the kind of people who are good at looking at big messy piles of data and detecting patterns that others are unable to see. That's the level of complexity we're working with.

I think there's a couple of different routes that should be explored. First, go really basic: say any post that is viewed more than 10,000 times (which is a very small fraction of posts because we never see 99.9% of posts), is no longer private.

What does private mean to you? If I send a message to a group chat with eight people, is that private? If I send it to 16 people, is that private? If I send it to two or four people, that's private. And the point at which people say, hey, if I post it to a forum that has more than 32 people, it's no longer private. I don't have privacy.

That kind of makes sense when you think about humans. You know, you can imagine being in maybe a self-help group and that group might have 20 or 30 people and you could still feel like there was an intimate conversation, but you get on to a larger sphere and people don't have an expectation of privacy anymore. Setting a 10,000-view limit pushes us to understand the biases of the algorithm. What are they amplifying the most?

I think most Europeans aren't aware that Facebook does have a transparency report that shows the most viewed content on its platform. However, it only shows the top 20 posts in English, from the US, once a quarter. When you put all of those qualifiers in, you have to ask: why? Only 8-9% of all Facebook users are in the US–so why constrain the report only to the US?

The reason the reports are done for English content alone is because the safety systems are overwhelmingly built for English, for American users–not for people elsewhere.

If any post that hits 10,000 views in Europe was published in a weekly dataset, we could very quickly apply very complicated analysis to understand disparate impact: Does content for minorities get distributed on the platform? Who gets targeted with what kind of information? Are we seeing hotspots where people and groups are shown more violent and socially destabilizing content, more content tied to self-harm, or content that might have serious health consequences?

Gaining access to even that tiny window would change everything–because right now, we see nothing, and the consequences are enormous. The reason why this is so fundamentally important is because even the most cursory of examinations of the data would showcase the kinds of topics are blacklisted, suppressed, and ignored.

As long as social media operates under the current profit incentives, is there a way to prevent the inherent privacy trade-offs of giving up personal data for convenience in digital spaces?

People sometimes say that they need a law that gives us the right to opt in or out of having their personal data used by these companies. But I've always observed that these companies have no interest–and no incentive–to make your experience even mildly enjoyable if you don't give them your data.

People like algorithmic feeds. They like personalization. They may have concerns about it, and they may wish they could reset it occasionally, but they like it. Failing to address and acknowledge the reality that people like personalization makes it impossible to understand how to have a meaningful conversation when it comes to privacy.

For other technologies–like the phone or the computer we use to communicate with one another–competitive market forces have induced improvements and development. Third-party reviewers test and benchmark devices to tell you how reliable it is, which users can access and use to inform their decision on whether they should or shouldn't buy the product. The feedback loop and informed decision-making it encourages serves to keep the suppliers of these technologies honest, and helps them make a better computer next time.



Because in a world where they can accumulate information on you, you can end up in a situation where your view of reality becomes very, very tailored. All that information they've collected is used to influence what you're allowed to consume.

But with social media, we have so few facts on how the systems are built, what they do with our data, what they do with the people, and who uses it. We don't get to make real choices. What we can do is put pressure on these companies and say: "We are making these kinds of investment decisions going forward, over time. You can participate–or you can be left behind.

Around the world we've seen youth advocates working to reclaim social media spaces to put the "social" back in social media again to have a human-centric design. What advice would you give to younger generations to support that movement?

I think one of the most powerful things you can do is read history. That is the thing that gives me the strength to continue talking to advocates, legislators, and students. All because it happens very slowly.

Think of the 20th century: the Soviet Union fell and the British left India. Things that once were considered absolutely impossible eventually happened. Social media platforms have no incentive to change, and so won't change on their own. But we can and we must change their incentives–which is how all big systems eventually ended up falling.

One of the things that I really want to emphasize, especially for young people in Europe: a new social platform begins with just two users. It's spaces that we build that we choose to spend our time in.

One of the most transformative things that we can do is to have more conversations with young people–even going all the way down to elementary school. Ask them: Why do you use these platforms? Ask these kids if they would choose to spend their time somewhere else, in other spaces, if their friends went too?

Because we can't count on the US anymore and we can't count on corporations to shape our reality, not if we want to live in a future that is about people, not profit. ▪

Interview with

Frederik De Wilde

We gladly introduce the CPDP net-Artist in Residence, working at the intersection of art, science, technology, and design. His practice explores the inaudible, intangible, and invisible in digital and physical spaces, critically engaging with the societal and environmental shifts driven by technology. De Wilde's work navigates speculative futures and complex systems, offering innovative perspectives on contemporary challenges.

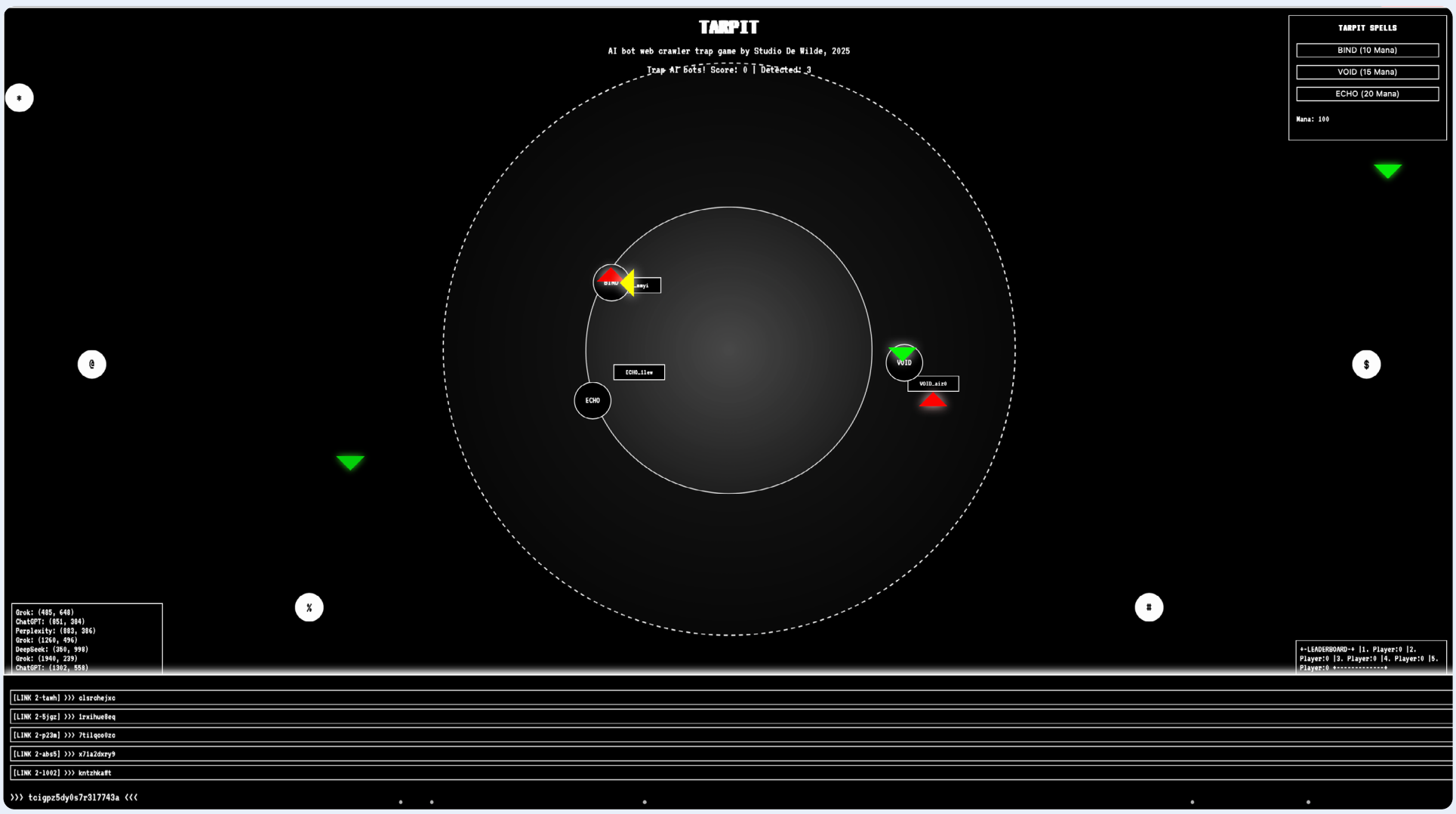
Frederik, I classify you under the trans-disciplinary artists moniker. When I got to know you and your work sometime around 2003 in Brussels, you were playing around with the modular Max/MSP music composing program, creating compositions. Simultaneously you worked on a movie, which was short and creepy and had some interesting David Lynch qualities. During the years, the number of collaborations you had with technology researchers continued to increase. You developed the Blackest-black with nano technology. Your fascination with the web and web-based art is clear to me. You still do that: working on 20 projects simultaneously. Can you quickly explain what your project about the dark web is about and how it is developing?

There's a backstory, of course: a few years ago, I was fascinated by the dark web, or dark- net. We live on the surface web and then you have the deep web (everything in between), and finally the Darknet, the lowest level of the internet. I was curious how to access it. I used Tor to explore this hidden, obscure space. It's a kind of spectral landscape of whistleblowers and the military, because that's the origin of the internet itself, to understand its origins. In fact, I discovered it's not an exciting place at all. It's extremely boring, right? Because you can't find almost anything. You really have to take a lot of time, deep dive, and infiltrate networks to discover something. But on YouTube, you can find some stuff that surfaced from the Darknet. One thing that drew my attention was *Sad Satan*, a Darknet-only horror game (until now). It's made with a custom 3D engine called Terror Engine, which created a lot of fuss years ago on YouTube because it's a game without logic. Normally in a game, you have to complete tasks to get rewards and all that. But this is like a Lynchian, nonsensical game using conspiracy theory images or sounds that are linked to serious crimes. It was provocative. That's why everybody wanted to see it, and that tells me something about the nature of people, of mankind. We're drawn to these dark spaces, fascinated by the unknown and all that. So that was my internal drive to explore it all. Then I scraped some videos and material from the Darknet and created an experimental video. But in a nutshell, after that video I applied to the VAF (the Flemish audiovisual film institute) to make a more elaborate version. When writing the narrative for a single screen, though, I realised: it should be immersive. You want to be immersed in the Darknet directly, not just look at a representation. I opted to move from a film to VR, and that's how *Alice in Darknet* was born. Right now, we have a playable proof of concept. I'm currently talking with publishers, gaming companies and so on to create a fully revamped version, but as a game, not just an immersive experience. That's the current stage.

You also recently made an interesting installation about mineral extraction in function of tech development, can you tell us about this?

It was a work I developed during the COVID period, after an open call from a Foundation in Greece and the United States to explore concepts through the lens of artificial intelligence. I've always been deeply interested in mineral extraction given its current geopolitical relevance. I made this in real time, and it's completely programmed in an interactive environment like TouchDesigner, a triptych. In the first

When writing the narrative for a single screen, though, I realised: it should be immersive. You want to be immersed in the Darknet directly, not just look at a representation.



TARPIT | © Frederik De Wilde

(real-time) animation, a satellite orbits Earth, scanning for valuable resources using hyperspectral imaging. The second one shows orthogonal Google Earth images, with AI identifying deposits. The third reveals a new geode—a rebuilt Earth with the valuables the AI found. That's why the project is called *Hyperminer Extracted Earth:* serving as both a critique of extractivism and the Anthropocene.

We invited you to become a net artist-in-residence at CPDP.ai. Exciting! Can you tell us what the plan is and a little more about the TARPIT project?

It's not the first time I've explored counter-tactics and counter-surveillance strategies. I already explored this a little with my AI Beetles project, and trying to fool AIs, a pioneering collaboration with the University of Wyoming's AI Lab years ago. But I never explored it in relation to AI agents, because Genentech AI is quite recent. These agents are bots that basically scrape websites and anything else -- think about DeepSeek, ChatGPT, and similar tools. So, I was thinking: *how can we connect these ideas?* Create something browser-based, a gamified environment. Basically, a website that's both a game and a trap, a primitive trap that is playable by users. The goal is to hypnotise AI agents, luring them into an endless loop. I find it really fun and interesting because it's not just art. It's not a game. It's also cybersecurity. You really have to understand all the tactics and strategies of cybersecurity. But then I try to go a bit further than what most cybersecurity specialists would. I'm reading Roger Caillois, the French sociologist who wrote *The Mask of Medusa,* about relationships between insects, animals, and humans, and their camouflage techniques which are strategies that exist in both worlds, and I'm drawing a lot of inspiration from this to see how it could change my perception on strategies. I'm now looking into ancestral knowledge and spells and exploring how to create new kinds of traps based on ancient spells. I really like this surrealist, absurd fantasy element. Finally, MC Escher's work is another inspiration. He's known for his labyrinthine structures that are nonlinear, like *Sad Satan.* They share that particular complexity, hard to encrypt or decrypt. These architectures are themselves recursive loops, endless loops you can't escape. I find this especially fascinating in digital and web space, a hyperdimensional realm that extends beyond visible pixels. The project has a lot of depth and so much to excavate and discover. As an artist, my first goal is to understand how cybersecurity strategies and tactics work, then explore what new input art, sociology, biomimicry, and so on can contribute. I want to see how this influences both the artistic process (how to nurture it) and the outcome.

As part of the residency, you'd like to collaborate with the CPDP community. You are present at CPDP, organising a session to engage the community. Can you tell me how you see that? How can they impact the residency and the Tarpit project?

Sharing knowledge, the process, and presenting my work is the opposite of what start-ups do. Let's look at an AI agent as a metabolic system or as a human. These agents aim to digest and consume *the honey pot* (a cybersecurity term), which the website contains. The problem for AI agents however, consuming websites is extremely energy-intensive, and so are the algorithms. These startups are now making websites pre-digested for agents, intervening before they even arrive. How do they do it? By translating everything on-screen into text, making it much easier for agents to digest. What I'm doing is the complete opposite, my approach serves as both provocation and precedent. Right now, everything's either attack or defense—you need both. You want to give users (individuals, whatever you call them) the ownership of their websites, deciding whether to allow scraping is an ethical consideration. This is responsible AI. Right now, it's the Wild West out there. This project aims to bring these questions to the table, to discuss how we'll handle this. What's happening is a form of post-colonialism, we must address this, and art is a great way to do it.

What impact do you hope Tarpit will have on debates about ethics, data extraction, open-source tools, AI bots, everything?

It will also depend on feedback from the scientists, the companies, Privacy Salon, and from everybody. It's a shared responsibility, an organic process - not merely setting a target and measuring impact. It could evolve in various directions. So, there can be diverse impacts. One principle of art is raising critical questions, creating interactive experiences. I don't want to be conclusive, but achieving this, while staying open to influence, and vice versa. I hope the game itself evolves—and that in the open-source domain, others can learn strategies and tactics, modify the source code, and build their own traps. I hope to see a zoo of different games that elaborate on what I've started. That'd be great. I see impact in the artistic sector, gaming sector, cybersecurity, and potential collaborations with companies. I'm open to that. So, I think the impact can be big. It really depends on both me and us collectively.

How do you feel Tarpit relates to this year's CPDP theme, 'The World Is Watching'? There's potentially much to unpack.

The World is Watching, is in my view a human-centric slogan, and we're in an age of non-human entities—a hyperconnected world of IoT, surveillance cams, hyperspectral cameras, everything becomes much more interlinked yet *fragmented* by geopolitics issues, so it is a very strange, confusing world. There's a rat race for the best technology and for richest natural deposits, to fuel these new economies and technologies. I think the world is watching this, raises the question: *who is truly watching?* And it's not just people. For me, that's the interesting thing—the dynamics that exists between humans and organisations. There's a lot to unpack. Think Orson Welles, 1984. But for me, it's about far more than surveillance, right? It's how everything becomes super entangled. It's not just watching, it's listening too. If you understand how large language models (LLMs) turn text to images, images to sound. So, is 'what is watching' still relevant? Is that still the right way to describe it? Watching is just one (intentional) sensorial aspect. There is also touching and feeling things, it becomes sentient. There is haptics already involved, smart skin that's touch-sensitive and connected; then there are brain implants that connect you to computers or monkeys. I mean, there are things going on right now that make me think we're entering this field of hyperobject, also the *concept explored* in Timothy Morton's book. When things become too difficult to fathom or too big, they *transform into* hyperobjects. So, for me, *'The world is Watching?'* is exactly that.

One more note: what you do is also visualising something that generally remains invisible to people. By visualizing the agents' passage through the net—through everything we do, you give civil society agency, letting them observe what's typically meant supposed to stay invisible?

I think about the connection between metabolism, the human body and viruses. Suddenly, you have both a looking glass and microscope, you're looking into the petri dish of your screen, observing the activity of these bugs, agents, bots. It all turns almost biological. That's fascinating. So, do you give people a tool to magnify, and make transparent the dynamics that are at play? This under stream allows them to interact with it, play with it and discover. It taps into *homo ludens* (the playing person), to discover these technological infrastructures and dynamics through playful engagement. Personally, I find that to be a very good approach. ▪



As an artist, my first goal is to understand how cybersecurity strategies and tactics work, then explore what new input art, sociology, biomimicry, and so on can contribute.

Organisation of CPDP

Directors

- Paul De Hert (LSTS, VUB, Tilburg University TILT)
- Dara Hallinan (FIZ Karlsruhe GmbH - Leibniz Institute for Information Infrastructure)
- Thierry Vandenbussche (Privacy Salon) Interim Director
- Jonas Breuer (CPDP - Belgium) Interim Director
- Joren Baillière (PS - Belgium) Interim Director

Core Programming Committee

- Paul De Hert (LSTS, VUB, Tilburg University TILT))
- Jonas Breuer (CPDP - Belgium)
- Dara Hallinan (FIZ Karlsruhe GmbH - Leibniz Institute for Information Infrastructure)
- Carissa Anderson (Privacy Salon)

Extended Programming Committee

- Luca Belli (Center for Technology and Society at FGV Law School)
- Ronald Leenes (TILT, Tilburg University)
- Dennis Hirsch (Ohio State University Moritz College of Law)
- Omer Tene (goodwin)
- Malavika Jayaram (Digital Asia Hub)

Panel Coordinators

- Achim Klabunde (Deutsche Vereinigung für Datenschutz DVD)
- Adriana Schnyder (undefined)
- Alessandra Calvi (d.pia.lab, LSTS, VUB - Europe)
- Andrés Chomczyk Penedo (undefined)
- Birte Vingerhoets (Privacy Salon - Belgium)
- Carissa Anderson (Privacy Salon)
- Dara Hallinan (FIZ Karlsruhe GmbH - Leibniz Institute for Information Infrastructure)
- Francesca Tassinari (Juan de la Cierva (JDC))
- Guillermo Lazcoz Moratinos (CIBERER)
- Isabel Sola (Alight Solutions)
- Isabela Xavier Gonçalves (Vrije Universiteit Brussel (VUB) - Belgium)
- Jonas Breuer (CPDP - Belgium)
- Joren Baillière (PS - Belgium)
- Josipa Špoljarić (IAPP-designated Certified Information Privacy Professional for Europe (CIPP/E)
- Lucas van der Horst (Fraunhofer Institute for Integrated Circuits)
- Naira Lopez (Technological University of Dublin)
- Nonso Anyasi (University of Bradford and CPDP Africa - International)
- Wenkai Li (LSTS (VUB)

Scientific Committee

- Gloria González Fuster (LSTS/VUB - Belgium)
- Rocco Saverino (ALTEP DP - Belgium)
- Franziska Boehm (FIZ Karlsruhe GmbH - Leibniz Institute for Information Infrastructure - Germany)
- Eleni Kosta (Tilburg University - Tilburg Institute for Law, Technology and Society (TILT) - Netherlands)
- Ian Brown (Fundação Getulio Vargas Law School, Visiting Prof - Spain)
- Ronald Leenes (TILT, Tilburg University)
- Paul De Hert (LSTS, VUB)
- Dave Lewis (ADAPT Centre, Trinity College Dublin - Ireland)
- Willem Debeuckelaere (Former President, Belgium Privacy Commission)
- Eva Lievens (Ghent University - Belgium)
- Claudia Diaz (Nym Technologies SA)
- Jo Pierson (VUB)
- Michael Friedewald (Fraunhofer ISI - Germany)
- Kristina Irion (Institute for Information Law (IViR) - Europe)
- José Luis Piñar (Ada Lovelace Institute - International)
- Charles Raab (University of Edinburgh - United Kingdom)
- Marit Hansen (State Data Protection Commissioner of Land Schleswig-Holstein)
- Marc Rotenberg (Center for AI and Digital Policy (CAIDP) - International)
- Mireille Hildebrandt (LSTS (VUB))
- Ivan Szekely (Central European University/ Blinken OSA Archivum - Hungary)
- Dennis Hirsch (Ohio State University Moritz College of Law)
- Gus Hosein (Privacy International - United Kingdom)
- Frederik Zuiderveen Borgesius (Radboud University - Netherlands)
- Els Kindt (CiTiP)

Privacy Salon

- Thierry Vandenbussche
- Jonas Breuer
- Joren Baillière
- Karin Neukermans
- Christel Simons
- Ferre Vander Elst
- Birte Vingerhoets
- Carissa Anderson
- Daria Ermolovich
- Jiao Feng
- Tija Gruden
- Ayse Darakçi
- Dongshu Zhou

Logistics and Registration

Medicongress Services

Noorwegenstraat 49
9940 Evergem Belgium

Phone: +32 (09) 218 85 85
www.medicongress.com

Auvicom

Suikerkaai 40d
Zone 3a, 1500 Halle Belgium

Phone: +32 2 2 380 10 44
www. auvicom.be

Studio Pompelmoes

hello@bartvandersanden.be
www.studiopompelmoes.be

Josworld

Rue de Laeken 99
1000 Brussels

jos@josworld.org
Phone: +32 2 411 20 54
www.josworld.org

Thank you

This conference would not be possible without the industrious support of Els Vertriest, Sofie Philips, Ariëlle Desmet, Astrid Dedrie and all Medicongress staff, as well as the technical support of the wonderful people at Auvicom, in particular Joseph Cuvelier. Also, for the mastery of our caterer Les Frères Debekker, a big thank you to their team for providing such delicious food! A big thank you to Jean Vandamme for the great partnership between CPDP.ai and Maison de la Poste. A big thank you to Martine Renwart and her colleagues from Le Baixu, and Julie Posschelle and the staff from Brasserie de la Senne who are hosting the CPDP Party on Thursday.

To the Privacy Salon team for all the great work behind the scenes of CPDP.ai: directors Thierry Vandenbussche, Jonas Breuer and Joren Baillière and their team: Karin Neukermans, Dara Hallinan, Christel Simons, Ferre Vander Elst, Birte Vingerhoets, Carissa Anderson, Daria Ermolovich, Jiao Feng, Tija Gruden, Ayse Darakçi and Dongshu Zhou. Also a big thank you to the Privacy Salon board members for their guidance: Paul De Hert, Rosamunde Van Brakel, Ulrich Seldeslachts, Marleen Wynants and Jo Pierson.

Many thanks also to all LSTS and student volunteers who have done a wonderful job, and a particular thanks to Manos Roussos from Tilburg University who very capably managed the call for papers and academic sessions.

Special thanks to all of our Workshop Partners, who helped us make these dynamic, hands-on sessions.

A big thank you to Thierry Vandenbussche, who commissioned the cover artwork by James Bridle for CPDP.ai 2025 and brought 'The World is Watching' into the CPDP.ai sphere. Bridle is not the only artist at the conference, the CPDP Culture Club is full of inspirational artists and creatives who we would like to thank for their time and generosity. The CODE project brings an interesting selection of artist and non-artists who are collaborating and presenting projects together at the conference. Thanks to the collaboration with Impakt, Werktank, Kunsthal Mechelen, Arjon Dunnewind, Pietro Ballero and everyone involved in CODE. With Avatar.fm we make live radio from the conference for the second time, this year with radio station DubLab and the professional guidance by Joscha Creutzfeldt.

Thank you, Laura Drechsler, Aurélia Tamò-Larrieux, Irène Kamara, Anastasia Karagianni, Daniel Solove, Maria Magierska, for helping to organise the third edition of the CPDP Book Club. Thank you, Iris Stroep, from the local Antwerp bookshop De Groene Waterman for bringing an excellent selection of books to CPDP.ai 2025.

We're also especially grateful to Helen Nissenbaum and Yan Shvartzshnaider for bringing the Contextual Integrity Symposium to Europe for the first time. Huge thanks to August Bourgeus and Ine van Zeeland (imec-SMIT, Vrije Universiteit Brussel), Prof. Jo Pierson, the Brussels Privacy Hub team, and many others who made the Symposium possible.

The Digital Rights Lounge – Powered by Privacy Camp has been made possible as another valuable pre-event to CPDP by a passionate group of people: Ella Jakubowska, Claire Fernandez, Guillermo Peris, Gloria Gonzalez Fuster, Rocco Bellanova, Michael Sewell, Birte Vingerhoets, Carissa Michelle Anderson, Thierry Vandenbussche and the amazing people from BeCentral.

Thank you to Gianclaudio Malgieri and Mireille Hildebrandt, for making the CPDP.ai Opening Night a strong and thought-provoking start to the week—and to the Brussels Privacy Hub and Privacy Salon for sponsoring the adjoining cocktail. We also warmly thank the EDPS, the Center for Future Generations and CAIDP Europe for sponsoring the evening cocktails on Wednesday, Thursday and Friday respectively.

CPDP is grateful towards Dara Hallinan, Paul De Hert, Eleni Kosta and Suzanne Nusselder, as well as Roberta Bassi and Rosemary Mearns from Hart Publishing, the academic contributors and the editors of the conference book who did a great job again. As with every year, they have produced a book of high value which leaves written proof of what CPDP.ai is: an ambitious bet to knock down barriers among disciplines, think together, innovate, and leave a mark in the privacy and data protection world.

Thank you also to our brilliant team of reviewers for the CPDP.ai 2025 call for papers, all those involved in the process leading to the CPDP.ai 2025 conference book, and the reviewers for the academic sessions: Tjasa Petrocnik, Jonas Breuer, Damian Clifford, Tynke Schepers, Masa Galic, Max Van Iersel, Irene Kamara, Gergely Bizcok, Ashwinee Kumar, Gianluigi Riva, Pawel Hajduk, Michael Friedewald, Arnold Roosendaal, Maria Murphy, Marco Bassini, Manos Roussos, Burak Özdemir, Joren Baillière, Colette Cuijpers, Giovana Lopes, Noelle Ann Park, Brenda Espinoza Apraez, Shweta Degalahal, Alexandra Ziaka, Ine Van Zeeland, Ian Brown, Ivan Szekelyi, Joseph Savirimuthu, Linnet Taylor, Stephanie von Maltzan, Gabriela Fortuna Zanfir, Iraklis Symeonidis, Suzanne Nusselder, Aleecia McDonald, Inge Graef, Mindy Duffourc, Joseph Savirimuthu, Shakya Wickramanayake.

We are grateful to the first-ever curators of the Computer Science and Data Protection Officer (DPO) Tracks, for their expert advise and availability throughout the year when completing the CPDP Tracks. Thank you, Jaap-Henk Hoepman, Marit Hansen, Peter Berghmans and Jolien Ghyselinck.

Additionally, we would like to thank all the panel liaisons for facilitating communication between the Programming Committee and the panel organizers. In particular Achim Klabunde, Adriana Schnyder, Alessandra Calvi, Andrés Chomczyk Penedo, Birte Vingerhoets, Carissa Anderson, Dara Hallinan, Francesca Tassinari, Guillermo Lazcoz Moratinos, Isabel Sola, Isabela Xavier Gonçalves, Jonas Breuer, Joren Baillière, Josipa Špoljarić, Lucas van der Horst, Naira Lopez, Nonso Anyasi, Wenkai Li.

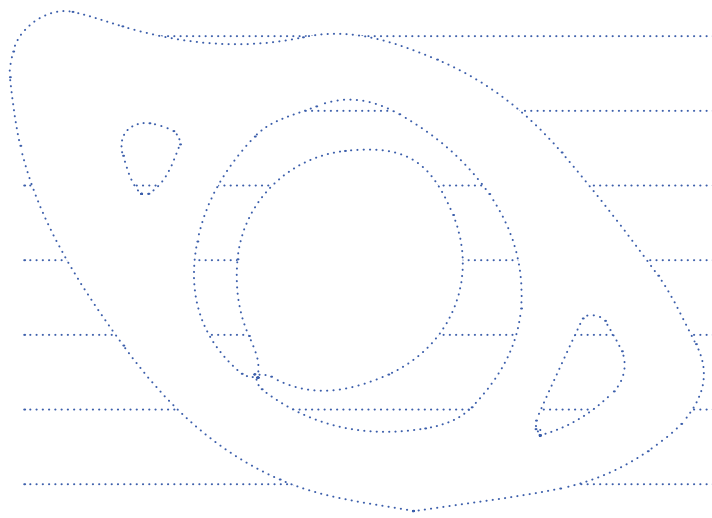
Furthermore, we would also like to thank Dongshu Zhou for his excellent coordination of the conference rapporteurs. We are also grateful to the rapporteurs themselves: Iris Karoli, Sofia Llull, Neha Tamil Selvan, Maria Nawara, Ine van Zeeland, Noa Daryn, Laura Mairal Sampedro, Miruna-Gianina Cojocaru, Adam Sereir, Severin Engelmann, Ezgi Ercan, Ishitaa Narwane, Cesar Fontanillo and Lyubomir Nikiforov.

Thank you to Kathleen Verbesselt and Agnieszka Piotrowska from Josworld for your incredible creativity and dedication, your work has truly brought this magazine to life. This publication would also not have been possible without the coordination of Birte Vingerhoets and the support of her editorial team: Thierry Vandenbussche, Joren Baillière, Carissa Anderson, Jonas Breuer, Ferre Vander Elst and Ayse Darakçi, for thoughtfully composing the interview questions, carefully editing the transcripts and creatively curating the content.

A special word of gratitude goes out to Bart Vander Sanden, our web-master and graphic designer, whose quality work – including the new website – is evidence in itself, and who we have additionally gotten to know as a hands-on and energising addition to the CPDP organising team.

And of course, to the CPDP.ai Scientific Committee, who steer and ensure the academic rigor of the conference programme. Last but not least, the Programming Committee of CPDP.ai2025 would like to thank all sponsors, conference partners, event partners, moral supporters and media partners for their generous support and everyone who has approached us with new ideas and topics for panels. Without you CPDP.ai 2025 would not have been possible!

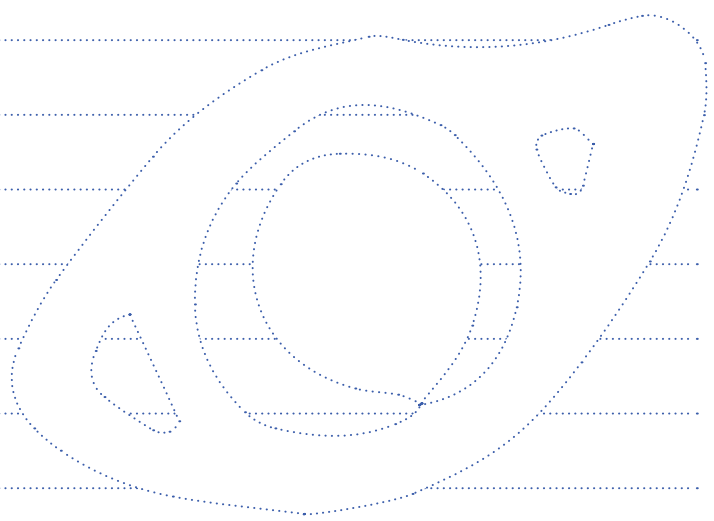
Notes



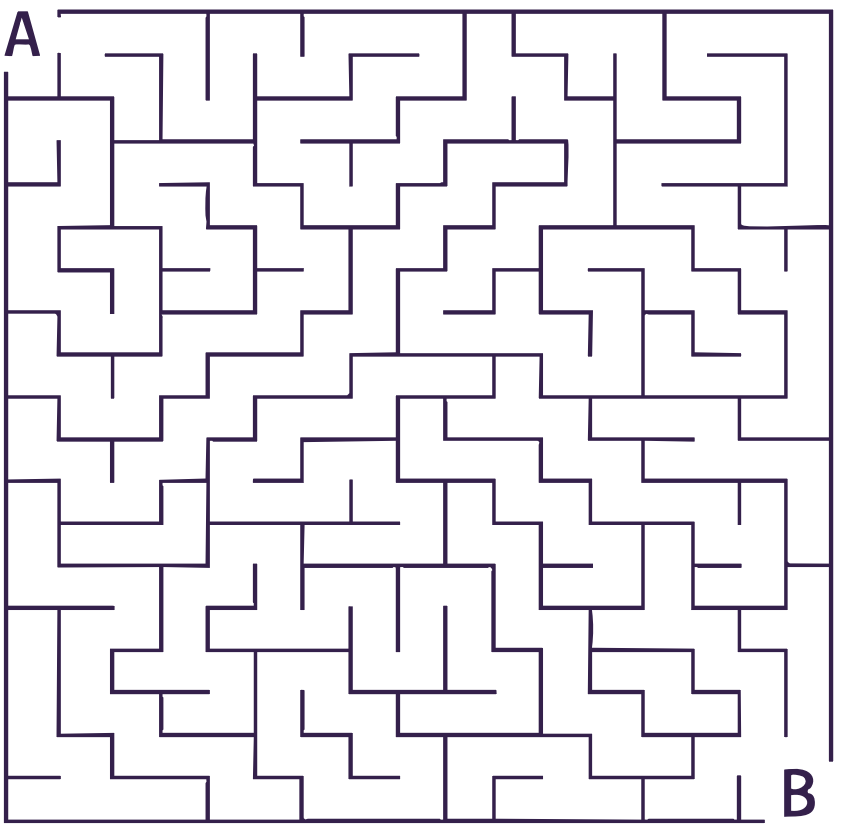
How observed do you feel right now?

- **4** Intensely observed
- **3** Moderately observed
- **2** Subtly observed
- **1** Silently observed

Notes



Go from point A to point B in this AI-generated maze



Sponsors 2025

Platinum

Premier

Event

Partners 2025

Conference Partners

Event Partners

Media Partners

Moral Supporters

CPDP.ai sponsors are organisations committed to dialogue around privacy, data protection and new digital technologies. Their contributions help to make CPDP into a trusted, quality conference that attracts participants from all over the globe. No more than 49% of the costs for the conference is covered by private enterprises, ensuring that commercial CPDP sponsors maintain an exclusive position in the privacy and data protection community.