CPDP 2026
Session Reports

Day 2

With thanks to our rapporteurs.

The reports are prepared independently by CPDP rapporteurs and reflect their understanding and interpretation of the sessions they attended. The reports are intended as summaries rather than official transcripts or records of the discussions.

CPDP 2026
19th international conference
19-22 May ■ Brussels, Belgium
COMPETING VISIONS, SHARED FUTURES

Designing Collective Technology Governance

Date: 21 May 2026

Panel Organiser: Max Planck Institute for Security and Privacy

Moderator's Introduction

Asia Biega opens the discussion by stating that contemporary technology governance frameworks are no longer adequate to address the current problems. The current technology governance frameworks are predominantly individualistic, while data about individuals is deeply interconnected through machine learning systems, such that decisions concerning one person's data can affect others. Moreover, many harms associated with algorithmic systems are not merely individual but structural in nature. This panel examined whether the growing mismatch between individual-centred governance frameworks and the collective character of contemporary technologies can be remedied through incremental reforms or whether it necessitates fundamentally new approaches to governance.

Panellists' contributions

Jane Suiter, Dublin City University

Jane Suiter starts with the argument that effective technology governance requires collectively agreed baseline principles rather than superficial forms of public consultation, as these consultation processes can be a performative 'tick-box' exercises that fail to produce meaningful democratic engagement. Thus, she advocates deliberative governance mechanisms, such as citizens' assemblies and juries, in which affected individuals collectively examine evidence and formulate shared principles. Jane Suiter also highlights the unequal influence of powerful corporate actors within governance spaces. Particular emphasis is placed on ensuring that marginalised and disproportionately surveyed communities are adequately represented, given that they are often most affected by data extraction and surveillance practices. She concluded that democratic legitimacy in collective governance depends on independence, transparency, inclusiveness, and clear institutional pathways linking deliberative processes to actual decision-making and regulation.

Kristina Zenner, BFDI

Kristina Zenner states that collective technology governance is a complementary approach that introduces mechanisms such as collective bargaining and structural representation for marginalised groups. However, she notes that collective governance cannot replace individual rights; rather, it should coexist with them to address the limitations of individual-centred regulation. Kristina Zenner also identifies major risks associated with collective governance, including unclear accountability, domination by powerful technology corporations, and limited transparency in collective decision-making processes. To address these concerns, she proposes safeguards such as co-regulatory legal frameworks, fiduciary responsibilities, institutional representation of vulnerable groups, and formal veto mechanisms to protect minority interests. Technical tools, including auditable systems and traceable decision-making processes, are also considered essential for ensuring transparency and regulatory oversight, though these tools alone are insufficient and cannot serve as a complete solution to governance challenges. Ultimately, the central objective is to develop collective governance structures that strengthen democratic legitimacy and collective protection while preserving fundamental individual rights and preventing power asymmetries.

Nicholas Vincent, Simon Fraser University

Nicholas Vincent discussed the emerging forms of algorithmic collective action, in which users collectively leverage their data to influence AI systems and technology companies. As AI increasingly depends on large-scale training data, users may gain new forms of power by collectively altering or withholding their digital behaviour to affect recommendation systems, search engines, or generative AI models. These developments are presented as complementary to traditional labour and political power, creating possibilities for new forms of collective bargaining centred on data and digital traces. Nicholas Vincent also argued that many technological governance challenges are fundamentally socio-technical rather than purely technical, requiring attention to social interaction, community dynamics, and democratic participation. Rather than inventing entirely new systems, researchers are increasingly adapting existing online platforms and interfaces to support deliberation, cooperation, and collective decision-making within digital communities.

Six Silberman, University of Oxford and International Trade Union Confederation

Six Silberman focuses on collective data governance in the workplace. He starts with an example of workers pooling their personal data obtained through GDPR data subject access requests. By combining and analysing these datasets, workers and researchers can identify patterns of inequality and challenge corporate narratives, as illustrated by the case of Uber drivers in the UK, where pooled data revealed declining worker pay despite the company's claims to the contrary. Six Silberman argues that such practices can strengthen labour advocacy, although emerging legal proposals may attempt to restrict these forms of collective data use. The discussion also emphasises that collective governance is fundamentally a political and social process involving power struggles, representation, and internal disagreement. Finally, he contends that meaningful participatory governance requires the capacity to build independent technical infrastructures and alternatives, rather than relying solely on proprietary systems controlled by large technology corporations.

Summary of Q&A discussion

Question 1: A privacy lawyer from the Netherlands: Since data protection law was originally designed to protect individual rather than collective rights, aren't alternative legal frameworks such as freedom of information laws more appropriate for achieving collective accountability and transparency?

Answers:

Six Silberman: The short answer is yes. However, the problem is political, as employers don't want to provide this information because, for them, it's a matter of power and control. This is the reason why workers have to do so.

Question 2: How can collective data governance adequately represent both current and former contributors whose data continues to persist and shape AI systems and organisational practices over time? Is there any research in this area?

Answers:

Nicholas Vincent: Yes, for example, data value estimation research aims to quantify the impact of different data contributions by assigning scores to data units in order to assess how collective action might affect algorithm performance.

Question 3: How can collective governance ensure that marginalised and vulnerable communities are not overshadowed by majority voices when platform harms affect different groups unevenly?

Answers:

Jane Suiter: Collective governance must ensure meaningful inclusion and representation of all affected groups, particularly marginalised and less powerful communities, so their voices are not drowned out or merely tokenised in decision-making processes.

Six Silberman: It is important to recognise that any collective representative body constitutes a form of power and must therefore be subject to the same accountability mechanisms used to oversee other powerful institutions.

Nicholas Vincent: Recommender systems and large language models can be understood as collections of parameters that are continuously shaped by users' interactions, meaning that collective behaviour already functions as an implicit form of governance over these systems.

Question 4: Asia Biega (Moderator): What kinds of decisions can we apply collective governance to?

Answers:

Jane Suiter: Society should agree on broad collective principles for value-laden technologies, while allowing minor updates within those principles, since frequent changes (such as software updates) can undermine prior individual choices without meaningful consent.

Question 5: Do companies already incorporate some form of collective governance when doing user research and usability and getting feedback from users?

Answers:

Nicholas Vincent: Yes. Technology companies would conduct more representative user research and produce outcomes similar to those aimed at by regulatory or collective governance interventions. The current shortcomings are mainly due to broader societal issues rather than poor or insufficient user research by tech companies.

Jane Suiter: Tech companies primarily optimise for user attention and engagement rather than societal or ethical values, making internal user research insufficient. Therefore, external regulation is still necessary.

Question 6: How can AI tools be used in a way that is better aligned with the values and needs of specific institutions, particularly public research and education settings?

Answers:

Asia Biega: It is a question about how we translate our decisions into concrete technical design. Different communities employ different terminology to describe this challenge, for example, socio-technical alignment. However, regardless of the label, it remains an unresolved and highly contested problem.

Nicholas Vincent: It's about imagination. For example, a more constructive vision is that individuals occasionally engage with highly capable models to help design and build the non-AI tools and systems they wish to use.

Question 7: Asia Biega (Moderator): Who would facilitate collective decision-making and collective governance? Are there organisations that would take on this role?

Answers:

Kristina Zenner: While we may currently lack the capacity to implement such approaches at scale, sandboxes can provide valuable spaces for experimentation and learning.

Jane Suiter: Across Europe, democratic innovation is currently delivered by specialist practitioners working with governments, councils, and corporations. However, as societal challenges grow more complex, this capacity should be embedded within public services, civil services, and regulatory bodies.

Six Silberman: We should utilise Articles 40-44 of the GDPR.

Question 8: Asia Biega (Moderator): What should happen next so that collective governance could become a reality?

Answers:

Kristina Zenner: We should treat the current frameworks as first steps and examine how these methods can be expanded and adapted to determine their broader feasibility and potential.

Jane Suiter: An evidence-based conversation across multiple countries is needed. The Commission could play a leading role by convening a regulatory framework to articulate a shared vision for the future of AI regulation. The resulting principles and recommendations could then be disseminated across member states, fostering broader public deliberation.

Nicholas Vincent: One of the most promising avenues is through the lens of AI evaluation and safety. People should be open to multinational cooperation across traditional rivalries and power dynamics. Taking collective direct action via data leverage through a global framework is also a potential way.

Six Silberman: Take actions such as attending the International Labour Conference and working together on the platform convention.

Panel Questions

What forms can collective technology governance take, and what opportunities do they create?

In this panel, institutions such as citizens' assemblies, citizens' juries, collective bargaining, and structural representation for marginalised groups are proposed. Technologically, utilising collective data leverage to influence AI systems and technology companies is also mentioned. However, it is noteworthy that, in addition to superficial 'forms' of collective technology governance, a set of collectively agreed baseline principles is required to prevent such mechanisms from becoming merely performative exercises.

What socio-technical infrastructure can enable meaningful collective governance?

Several examples are mentioned in the panel. First, a robust socio-technical infrastructure requires the capacity to develop independent technological systems and alternatives, as relying exclusively on proprietary platforms controlled by large technology corporations is insufficient. Second, existing digital platforms and interfaces can be utilised to facilitate deliberation, cooperation, and collective decision-making within online communities. Furthermore, technical mechanisms, including auditable systems and traceable decision-making processes, can promote transparency, accountability, and effective regulatory oversight.

How can collective governance approaches achieve (legal) legitimacy?

Legitimacy in collective governance contingent upon principles of independence, transparency, inclusiveness, and clearly defined institutional pathways connecting deliberative processes to actual decision-making and regulatory outcomes. Specifically, a meaningful inclusion and representation of all affected groups must be ensured in the decision-making process. Moreover, even with the aim of collective protection, these approaches should always safeguard fundamental individual rights.

What are the risks and limitations of collective technology governance?

Several risks and limitations are mentioned in this panel. First, a collective governance mechanism can be a superficial 'tick-box' exercise without meaningful democratic engagement. Second, the actors involved in the governance mechanisms have unequal powers and

influences. Thus, marginalised groups can be underrepresented, notwithstanding their significant exposure to and impact from the issues concerned. Third, the decision-making process may lack sufficient transparency and have unclear accountability. Finally, a collective governance mechanism can never replace individual rights.

Moderator: Asia Biega, Max Planck Institute for Security and Privacy

Panellist 1: Jane Suiter, Dublin City University -JS

Panellist 2: Kristina Zenner, BFDI - KZ

Panellist 3: Nicholas Vincent, Simon Fraser University - NV

Panellist 4: Six Silberman, University of Oxford and International Trade Union Confederation - SS

Rapporteur: Ting-Yu Yu, the University of Edinburgh

CPDP 2026
19th international conference
19-22 May ■ Brussels, Belgium
COMPETING VISIONS, SHARED FUTURES

Exploring the lands of GDPR, DSA and DMA: Using the consent umbrella when it's raining with data

Date: 21 May 2026

Panel Organiser: Erasmus Center of Law and Digitalization, as part of Erasmus University Rotterdam

Moderator's Introduction

Larisa Munteanu opened the panel with a thank you to the organisation and the attendees and started the discussion with an initial question about the weak and strong points of consent as well as its associated challenges.

Panellists' contributions

Paloma Krõõt Tupay, University of Tartu

Paloma Krõõt Tupay was the first to answer the question by going over the aim of consent from a historical and legal perspective. She argued that, from its origins in the medical and ethical domains, it served as an expression of autonomy, that was imported into the legal domain, particularly for data protection in German caselaw. However, she questioned whether we are still capable of consenting nowadays against a more paternalistic approach where we are not allowed to consent and somebody else makes this decision for us. To illustrate this, she put the example of public administration relying on consent as a paramount of power imbalance that could compromise consent.

Felix Mikolasch, noyb

Felix Mikolasch followed the discussion by highlighting that the nature in consent in data protection is different to that of consent in contract law. As for the challenges to consent, the most difficult issue is that the requirement for a valid consent is presented in an abstract manner and the challenge lays in the application and interpretation of these provisions in concrete scenarios. These, according to him, have been mitigated through authoritative bodies delivering

advice and guidance, such as EPDB but also Member States data protection authorities. He then brought to the foreground other challenges such as the abundance of consent requests and whether this was fair under GDPR while stressing out the lack of enforcement due to potentially non-compliant situations.

Adrianus van Heusden, European Commission

Adrianus van Heusden moved the spotlight of the discussion towards the DSA and its intentions to create a fairer digital services ecosystem to support a more respectful implementation of consent-related practices. In this sense, he argued that the discussion around consent is meaningless if the structure around it does not protect users. As such, the systemic risk approach found in the DSA provides a valuable path to tackle issues pertaining to how these platforms are configured such as dark patterns. However, he also warned that, while these digital services provisions, would complement GPDR their actual scope of application is limited.

David Korteweg, Authority for Consumers and Markets in the Netherlands

Then, as David Korteweg took the microphone, he agreed with Adrianus van Heusden perspective on the role that rules such as the DSA play in delivering a holistic approach for users' protection, particularly for certain vulnerable collectives such as minors. He pushed the discussion one step further by question the reliance on consent as the default for enabling processing activities but also about the reliance on models such as pay-or-consent.

Larisa Munteanu, Erasmus Center of Law and Digitalization, as part of Erasmus University Rotterdam

Larisa Munteanu retook the microphone for another question for the panellists by first describing current consent practices and then asking for a reaction from them. Adrianus van Heusden agreed with the description presented and argued that consent without an actual possibility for choice is meaningless, citing the actions from Bits of Freedom against Meta over recommender systems. Paloma Krõõt Tupay also joined the discussion and highlighted that reality is far from the ideal purposed by GDPR where we find that consent is mostly unfree, ambiguous, etc. David Korteweg added as examples to build on Paloma Krõõt Tupay argument that of pre-ticked boxes and blanket provisions as examples of 'consent-washing'. Felix Mikolasch straight out called these practices as unlawful.

A third and final question was presented by Larisa Munteanu about how to solve this. Felix Mikolasch provided a first reaction by stating the automated signals as foreseen in the Digital Omnibus package were an initial good approach. David Korteweg argued that collaboration between enforcement agencies was absolutely necessary to address this matter with the existing legal framework, as the problem is not just about data protection but broadly about consumer protection and market regulation. Adrianus van Heusden joined this second analysis and added that answering which authority should tackle a given part of the problem was the first step towards meaningful enforcement.

Summary of Q&A discussion

The question from the audience revolved around four main topics: (i) the issue with ads relying on sensitive data and the role of consent in this situation after the Meta decision from the CJEU, (ii) the role of users to engage in litigation with digital services providers, (iii) addressing the actual sensible role of consent, and (iv) how to address the interplay between both regulatory authorities but also legal rules.

As for the first question, Felix Mikolasch and David Korteweg called for a careful analysis between the process, and therefore role of consent, for creating the group to whom a given ad is shown from the process of actually showing such ad to a person; Adrianus van Heusden argued that this legal developments mean that consent has a critical role to play in the attention economy.

The second question, mainly addressed by Adrianus van Heusden and David Korteweg; agreed with the analysis and called for authorities to pick up what users start from their enforcement capabilities.

The third question was answered by both Felix Mikolasch and Paloma Krõõt Tupay who considered that other legal basis has a bigger role to play but also require a more careful implementation, such as legitimate interest.

On the final question, mainly answered by Adrianus van Heusden and David Korteweg, was a repetition of the arguments raised for cooperation between authorities.

Panel Questions

What are, in your view, the strong and the weak points of consent across the GDPR, DSA and DMA?

Consent's primary strength across these instruments lies in its foundational grounding in personal autonomy, a concept imported from medical and ethical domains into data protection law, notably through German caselaw, that positions individuals as self-determining agents over their own data. The DSA adds meaningful structural reinforcement through its systemic risk approach, which addresses platform-level configurations such as dark patterns that undermine the conditions under which consent can be meaningfully given, complementing the GDPR's individual-facing consent framework. However, the critical weakness is that GDPR's validity requirements for consent are formulated at a high level of abstraction, placing the burden of interpretation on concrete application scenarios and creating endemic uncertainty that guidance from bodies such as the EDPB and national data protection authorities has only partially resolved. Further weaknesses include the sheer abundance of consent requests, which raises fairness concerns, and a persistent lack of enforcement against non-compliant practices, while the DSA's scope of application, though a positive structural addition, remains limited and does not fully cure the gap. The pay-or-consent model also came under direct scrutiny as a practice that calls into question whether consent as the default legal basis for processing activities is normatively appropriate.

Do you find the concerns you raised present only in private sector relationships or also in citizen-state ones? Please consider public-private partnerships too.

The concerns raised about consent are explicitly not confined to private sector relationships: the panel used the example of public administration relying on consent as an illustration of power imbalance that can fundamentally compromise the voluntariness that valid consent requires. This context is particularly significant because the power differential between a citizen and a public body is structural and difficult to overcome through design or interface choices, making consent an especially precarious legal basis in state-facing contexts. The panel further flagged that reality diverges sharply from the GDPR's idealised model of free, specific, and unambiguous consent, a problem that manifests across both private and public settings where consent is routinely unfree or ambiguous in practice. The DSA's user-protection provisions were acknowledged as relevant for vulnerable collectives such as minors, pointing to how the citizen-facing dimension of digital services creates intersecting private-public dynamics, especially where platforms operate in quasi-public roles. Cooperative arrangements between regulatory authorities, a theme that recurred in both the panel discussion and the Q&A, implicitly acknowledge that the structural problems of consent also arise in the hybrid spaces where public mandates and private service delivery intersect.

How would you describe, in up to 3 words, pre-ticked boxes and blanket consent applications? Please elaborate.

The panel characterised pre-ticked boxes and blanket consent provisions as instances of "consent-washing", a term introduced to capture how the formal vocabulary of consent is deployed to generate an appearance of lawfulness while the substantive conditions for valid consent are absent. These practices were also characterised as straightforwardly unlawful, a position grounded in the GDPR's requirements that consent be freely given, specific, informed, and unambiguous, none of which blanket or pre-populated mechanisms can satisfy. The broader analytical point is that reality has diverged substantially from the GDPR's normative model, with consent as it is actually practiced being mostly unfree and ambiguous, of which pre-ticked boxes and blanket provisions are symptomatic rather than exceptional cases. These mechanisms effectively deny users the genuine choice that the Bits of Freedom action against Meta over recommender systems illustrated as a necessary precondition for consent to be legally meaningful.

What are your recommendations for facilitating (or "simplifying ") the cross-regulatory stance of consent among these three legal instruments, if any?

The primary structural recommendation is that collaboration between enforcement agencies, spanning data protection authorities, consumer protection bodies, and market regulators, is an absolute necessity, given that the problem of defective consent is not reducible to data protection alone but cuts across consumer protection and market regulation as well. A prerequisite for such cooperation is first determining which authority is competent to address which dimension of a given problem, since the overlapping jurisdictions of GDPR, DSA, and DMA create coordination challenges that must be resolved before meaningful enforcement can occur. On the technical side, automated consent signals as envisaged in the Digital Omnibus package were identified as a promising first step toward operationalising consent in a way that reduces

the burden on users and limits the scope for consent-washing practices. The panel also implicitly recommended rethinking the default reliance on consent as the primary legal basis for processing, with other legal bases such as legitimate interest flagged as requiring a more prominent but carefully implemented role, suggesting that simplification may require reducing the normative weight placed on consent across all three instruments rather than merely harmonising its procedural requirements.

Moderator: Larisa Munteanu (Erasmus Center of Law and Digitalization, as part of Erasmus University Rotterdam – Netherlands) - LM

Panellist 1: Adrianus van Heusden (European Commission – Europe) - AH

Panellist 2: Paloma Krõõt Tupay (University of Tartu – Estonia) - PT

Panellist 3: David Korteweg (Authority for Consumers and Markets in the Netherlands – Netherlands) - DK

Panellist 4: Felix Mikolasch (noyb – Austria)- FM

Rapporteur: Andrés Chomczyk Penedo (Universidad Pontificia Comillas/Vrije Universiteit Brussel)

CPDP 2026
19th international conference
19-22 May ■ Brussels, Belgium
COMPETING VISIONS, SHARED FUTURES

The Russian Cyberpunk. How the Kremlin Builds a Digital GULAG — And Who is Resisting

Date: 21 May 2026

Panel Organiser: Andrei Zakharov

Culture Club Book Session

Moderator's Introduction

The moderator opened the session by introducing Andrei Zakharov's book, *The Russian Cyberpunk: How the Kremlin Builds a Digital GULAG and Who is Resisting It* (2025), which examines how virtually every piece of personal data in Russia can be purchased on an open market, and how the Kremlin has sought, with limited success, to bring this market under its full control. She framed the panel around the book's central paradox: that while Russia functions as a digital surveillance state, the same infrastructure also enables criminals, stalkers and investigative journalists alike to access the most sensitive data of both ordinary citizens and high-ranking officials. Ashurkevich situated the book within a cyberpunk rather than a purely Orwellian framework, noting that its cast of characters reflects a system defined as much by corruption and competing interests as by coherent state control. She structured the discussion around directed questions to the panellists before opening the floor to the audience. Ashurkevich ended with an acknowledgement of her own position as an investigative journalist operating outside Russia who is listed on Russian and Belarusian wanted registers.

Panellists' contributions

Andrei Zakharov, Independent Journalist

Andrei Zakharov opened by describing Russia's personal data market as unique globally. Drawing on his investigative work, he explained that data leaks are not only pervasive but commercially accessible through Telegram bots, where sensitive personal data, including addresses, border

crossings and financial transactions, can be purchased for the equivalent of ten cents. Zakharov illustrated this with a recent investigation into a deputy chief of the FSB, conducted using data obtained from a Telegram bot, only to discover that the FSB itself was purchasing data from the same source. He noted that police research reportedly found approximately 80 per cent of officers were buying data from such bots, and that Telegram had at one point provided free access to some officers upon receipt of an official letter. He argued that the market emerged from longstanding corruption: what began with illegal discs sold at city markets evolved into a digital ecosystem that the state both deplores and exploits, now a "Pandora's box" beyond state control. Zakharov framed the book's thesis through the lens of cyberpunk fiction: rather than a totalitarian dystopia of complete state omniscience, Russia more closely resembles a world in which corporations, criminal networks, and resistant actors, including investigative journalists, operate in the same grey market.

Daria Dergacheva, Independent Researcher

Daria Dergacheva offered a comparative perspective, arguing that Russia's experience with digital sovereignty and data surveillance carries important lessons for the European Union, primarily as a cautionary tale about where permissive data governance can lead. She noted that while many observers in Europe have criticised the GDPR as burdensome to business, the examples in Zakharov's book illustrate what life looks like without robust data protection, describing the dynamic as one of surveillance capitalism and surveillance authoritarianism operating in tandem. Dergacheva emphasised that data extracted from commercial platforms does not remain within commercial contexts, but feeds directly into mechanisms of state control and repression. She warned against the assumption that European democracies are immune to similar dynamics and argued that regulation should be evaluated not only in terms of its effect on industry but in terms of the protections it affords to ordinary citizens. She further argued that the EU had made mistakes by failing to regulate social media platforms early enough and called for greater attention to the citizens rather than to the competitiveness of European AI companies.

Olga Solovyeva, Researcher and Consultant

Olga Solovyeva provided a structural analysis of Russia's internet governance landscape, challenging the common characterisation of its digital control apparatus as a unified, monolithic system. When asked to rate the level of Russian internet control on a scale of one to ten, she offered a score of between seven and eight, noting that despite significant progress towards a closed system, many Russians continue to circumvent restrictions through VPNs and other tools, often provided by diaspora communities and exile organisations. She observed that Russia's trajectory is moving from a blacklist model towards a whitelist model for internet access and cited an NGO representative as estimating that a full internet shutdown could occur within approximately three years, though recent acceleration by the FSB might shorten that timeline. Solovyeva emphasised that the Russian political and security establishment should not be understood as a cohesive bloc, but rather as a collection of competing agencies and actors with divergent institutional interests, noting that the competition between different law enforcement agencies and the FSB is a structural feature discussed in Zakharov's book. She also drew attention to the economic incentives embedded at every layer of the data control system. Private companies with connections inside the state are monetising the system, while those involved seek to profit as quickly as possible. For Solovyeva, this gives the state more the character of a

poorly run start-up rather than a coherent state apparatus, making it simultaneously functional and corrupt. Solovyeva also reflected on Zakharov's book itself, observing that while Russia's early internet had been genuinely open and creative, the book documents what has been lost, and that the corruption and entrepreneurship it captures make it a particularly vivid account. She concluded by pushing back on uncritical use of the term 'digital sovereignty', arguing that without proper institutional support, the concept risks becoming an empty signifier that authoritarian actors can exploit for their own ends.

Summary of Q&A discussion

The Q&A was wide-ranging, drawing in the moderator as a participant alongside the panellists. The discussion covered the ethics of using illegally obtained data, the resilience of Russian society, and the relevance of Russia's experience for Western audiences.

The moderator asked all panellists about the biggest weaknesses in Russia's effort to build a system of digital control. Zakharov identified two: the structural difficulty of imposing a closed internet on a system built to be open and externally connected, illustrated by cases where attempts to block services inadvertently disrupted major banks, and corruption, since those tasked with building the system are simultaneously seeking to profit from it. He also pointed to the failed attempt to push citizens towards the state-affiliated messaging platform Max as an example of the limits of the Kremlin's ability to alter digital behaviour, noting that Max is part-owned by Putin's family, and that the arrangement reflects a broader Kremlin bargain in which political loyalty is exchanged for commercial comfort. Solovyeva added that popular resistance to state incursion into domestic digital life, visible during the COVID-19 pandemic and around military conscription, represents a genuine constraint on the system's reach.

The discussion turned to the ethics of using personal data obtained through illegal or grey-market sources in investigative journalism. Zakharov acknowledged the moral discomfort directly, noting that the same bots used in his investigations also enable stalkers and scammers, and that reporting on one such bot prompted its operators to take it offline, drawing complaints from other journalists who had relied on it. He described the situation as one of necessary dependence: in the absence of official access to data and in the presence of systematic state obstruction, purchasing data from Telegram bots remains one of the few investigative tools available. Moderator Ashurkevich stated that when investigating war crimes and the imprisonment of colleagues and friends in Belarus and Russia, she does not consider it unethical to use personal data relating to political actors who have chosen positions of power. Solovyeva characterised the practice as a form of self-defence. Dergacheva distinguished between the frameworks applicable to legacy media and those available to journalists operating under authoritarian conditions, suggesting exceptions may be warranted but must remain exceptions. Solovyeva intervened to challenge a potential assumption in the room, noting that not all Russians are politically passive or uniformly supportive of the state, and that many hold independent views but live within the reality of a repressive regime. She observed that forms of protest available in European democracies are simply not possible in Russia, and that where the Russian government crosses certain lines, society continues to push back in ways that are available to it.

An audience member asked whether Zakharov's book might function as a playbook for a new generation of activists. Ashurkevich responded affirmatively, while Zakharov was more cautious. The question prompted a broader exchange about the existence of cyber partisan groups, including Belarusian and Russian activists who hack government systems to obtain evidence of war crimes and provide material to investigative journalists. Ashurkevich confirmed that such groups exist, noting one small group of up to ten people that had reportedly hacked a Russian state institution.

An audience member raised the question of whether Russia's open data market could be seen as a form of democratisation of information, drawing a comparison with the Snowden revelations, where access was limited to a small number of state actors. Zakharov acknowledged the observation but noted that the same infrastructure powers epidemic-scale telephone fraud and targeted harassment, and that the accessibility of the data does not imply that its effects are democratic. Solovyeva cautioned against conflating the investigative use of data with its malicious use, noting that Russia's domestic repression and foreign disinformation campaigns operate through different mechanisms.

A final question from a student asked whether Russia's data market is a product of Putin's rule or a longer-standing structural feature. Zakharov responded that the market predates Putin, rooted in corruption and a historical absence of privacy culture, and that there is no single actor responsible for its existence. He warned European audiences by citing a proposed Swiss surveillance law, noting that Proton Mail's CEO publicly stated that the only other country with a comparable law was Russia. He added that many countries are travelling along the same path, and that civil society must be alert to the incremental normalisation of state access to data, however well-intentioned in the initial justification.

The panellists closed by converging on a shared message for Western audiences: civil society must resist ceding control over personal data to the state; frameworks such as the GDPR are hard-won protections that should be actively nurtured and defended; and Russia's experience demonstrates the concrete human cost of their absence. Zakharov noted that his perspective is inevitably shaped by personal experience, adding that both state surveillance and commercial surveillance represent threats to individual freedom, and that neither should be normalised.

Moderator: Tatsiana Ashurkevich, Independent Journalist - TA

Panellist 1: Andrei Zakharov, Independent Journalist - AZ

Panellist 2: Daria Dergacheva, Independent Researcher - DD

Panellist 3: Olga Solovyeva, Researcher and Consultant - OS

Rapporteur: Megan Leal Causton, Vrije Universiteit Brussel

CPDP 2026
19th international conference

19-22 May ■ Brussels, Belgium
COMPETING VISIONS, SHARED FUTURES

Like Moths to Light by Gala Hernández López + Cognitive Warfare w/ Virginia Mahieu

Date: 21 May 2026

Panel Organiser: Privacytopia

Culture Club Screening + Discussion Session

Movie Screening

The session began with a 27' screening of the English movie, 'Like Moths to Light'.

Synopsis: A woman talks to us from inside a machine that records her brain activity. She describes a mental labyrinth combining an old amusement park called Dreamland, 19th century dream photographs, contemporary experiments in mental de-coding using AI, and Prophetic, a start-up whose goal is to control dreams. But what do our dreams see when they look back at us? Like Moths to Light is a meditation on the future of our dream worlds in the age of neurocapitalism.1

In the discussion that followed, Hernández López described the film as something she conceived as a dream: fragmentary and non-linear rather than a conventional narrative, blending documentary and fiction, and built around a cautionary, Promethean arc (technology as the human substitute for the strength and speed of animals), that ends with the historical Dreamland destroyed by fire.

Moderator's Introduction

Departing from the film, Virginia Mahieu, Centre for Future Generations, opened by describing her background and a neuroscientist in the Thinktank CFG, where she maps Brain Computer Interfaces (BCIs), including what they are already capable of and what they could be capable of. She then described the diXerence between invasive (implanted in the body) and non-invasive neurotechnologies (wearable tech). Neurotechnologies have medical roots ranging from devices

[1] Taken from the o-icial synopsis of the film

like prosthetics to speech aid implants, some of which have amazing results. On the consumer side, the devices are simpler for now, measuring attention levels or fatigue. For example, they can measure brain sleep phases, like a smartwatch, but cannot (yet) decode what you are dreaming about.

Then she moved on to a deliberately dystopian scenario. Smart headphones detect that a listener is tired; at that vulnerable moment a social-media feed serves not merely a well-timed product advertisement but personalised emotionally provocative or politically manipulative content, while the same wearable measures the listener's reaction and feeds it back to the algorithm. Her central point was that none of these components is speculative: wearables, behavioural and neural profiling, generative AI and optimisation algorithms all already exist. What is still missing, she argued, is the ability to measure how content lands in the mind rather than merely tracking external engagement, and neurotechnology could begin to close that gap, opening the door to hyper-personalised persuasion and new possible forms of cognitive warfare.

She framed this as a warning: if we do not decide early where we want these technologies to go, and how to protect the data they generate, we risk new forms of cognitive intrusion. At the same time, she cautioned against both uncritical hype and pure fear. So, the task is to imagine how bad things could become precisely in order to steer toward where we actually want to land.

Panellist Contributions

Since this session only had the moderator and the filmmaker, this section focuses on the filmmaker's introduction.

Joining remotely, Gala Hernández López, Filmmaker introduced herself as an artist rather than an expert, who nonetheless undertook extensive research, like meeting neuroscientists at Harvard and across Europe, to discuss how real 'mind-reading' might be. One Spanish programme head she spoke to predicted fairly accurate decoding of mind content within ten to fifteen years.

Summary of Q&A discussion

Question 1: What was your inspiration behind the film?

Answers:

Hernández López explained that from the Prophetic article she assembled a constellation of historical and contemporary attempts to penetrate or decode dreams, travelled to film Coney Island in New York and the company, and then shaped the material through a voiceover written late in the process, into a dream-like work ending on the Dreamland fire as a cautionary myth for our ambition.

Question 2: Do you see, with enough regulation, a way forward where all the positives happen without people having to suNer in other ways?

Answers:

Mahieu stressed the technology's real benefits, especially in healthcare, and that although she remains an excited neuroscientist, the goal is balance. She pointed a white paper by her

organisation, recommending an EU neurotechnology strategy across three strands: (i) optimising the innovation and investment ecosystem, (ii) regulating marketing and unevidenced hype claims, (iii) and bringing the public into inclusive deliberation, given diXering public opinions, and limited public awareness of a fast-moving field. Her view was that Europe already has a wealth of regulation covering much of the technology, with remaining gaps would not take much to close.

Question 3 (by Hernández López): Why do people not care? How could we make people care about surveillance and privacy?

Answers:

Mahieu replied that the individual harms of such surveillance are very hard to connect to the systemic behavioural profiling they feed. She gave a personal example, while pregnant she was served not only baby-related content, but AI-generated podcasts apparently designed to sow fear in pregnant women, which has been linked to organised campaigns to destabilise vulnerable people. Seemed harmless at first glance, because it is relevant content, but can be dangerous. An audience member agreed that the harm seems abstract to grasp and related this to cookies on the internet.

Question 4: How to translate dreams to visual language into the film, where are you in the film?

Answers:

Hernández López conceived the whole film as a dream, dreams being fragmentary, absurd and non-Aristotelian, so that the viewer might feel, by the end, as though waking from one. Choices such as a diner the founder of Prophetic loved, a closing Coney Island cinema scene staging the audience as a collective dream, and a pulsating green light left deliberately unexplained were meant to invite each viewer's own interpretation. She also voiced a concern that, if such dream control technology succeeds, it could erode our similarity and make us more alike.

Question 5: On the film's recurring play of light and dark, reflecting the known and the unknown about the mind. In a sense the more we know, the less control we have over it. What is the thought process behind this?

Answers:

Hernández López: The theme of light and dark reoccurs through the film. She linked it to the Dreamland, an amusement park lit by electric light with the largest electricity contract in the US, and ultimately destroyed by fire when a lightbulb exploded, analogous to the Promethean myth. Furthermore, she linked it to a cultural dichotomy in which seeing and light is equated with knowledge, and progress and darkness with ignorance. She resisted that equation, arguing that there are things to see in the dark and that too much light can blind us; the film closes with its narrator realising she can see with her eyes shut. Her caution was against erasing all darkness and making everything visible, explicable, and exploitable, since parts of our being are not meant to be grasped in purely rational terms. Attempting to do so, with science, can result in a loss of meaning.

For Mahieu, the exchange echoed the cautionary tale of the fictional Jurassic Park, i.e., scientists being so absorbed in whether something can be done that no one asks whether it should be done. This for her, paralleled current debates about AI and chatbot-driven manipulation. Once the tech is here, it is hard to put back.

Question 6: On reaching the company Prophetic and its founder.

Answers:

Hernández López: She found the start-up through an article in Fortune Magazine. She was disturbed by the dystopian statement that we could spend the time we spend dreaming, working instead through lucid dreams. So, she contacted them, and went to New York to meet the founder (Eric). He was enthusiastic to be part of a film, the company was still raising funding, so in his view any publicity was good publicity and his on-camera material, including a speech delivered in front of an American flag, was unscripted and apparently already rehearsed for investors.

She read the company's pitch, dreams as a new frontier to conquer, through the American myth of the frontier while pointing to what that frontier narrative erases: dispossession and violence, and the unanswered question of who will own dreams once they become data.

Question 7: On the transatlantic split in neurotechnology.

Answers:

Mahieu: She described a divide her organisation has tracked in a study: in the United States, more investment flows to grey-area consumer and wellness products that make claims about what they can do for stress, anxiety, or migraines without much scientific evidence, often privately funded. In Europe, more activity is research-oriented and publicly funded. She tied this to an American cultural drive to push the frontier in the flashiest way possible, a drive Hernández López connected to a neoliberal, deregulated, and tech-founder atmosphere rather than to anything uniquely American in the Promethean impulse itself.

Moderator: Virginia Mahieu, Centre for Future Generations - VM

Filmmaker: Gala Hernández López, Filmmaker - GHL

Rapporteur: Kimmy Shah, VUB

CPDP 2026
19th international conference

19-22 May ■ Brussels, Belgium
COMPETING VISIONS, SHARED FUTURES

"My Chatbot, My Confidant?" Protecting User Privacy in Generative AI Conversations

Date: 21 May 2026

Panel Organiser: AI.REGULATION.COM Chair, MIAI, University Grenoble Alpes

Moderator's Introduction

Moderator Theodore Christakis opened the session by highlighting the growing role of generative AI chatbots as spaces for intimate and highly personal disclosures. Users increasingly share health concerns, relationship problems, legal questions, and other sensitive information with AI systems, often revealing information they may not share with friends or family. He noted that the conversational interface of chatbots encourages expectations of confidentiality, empathy and trust, while raising important questions about how these interactions are collected, stored, used and potentially disclosed. Christakis emphasised concerns relating to third-party access, law enforcement requests, and the possibility of identifying individuals through prompt histories. Against this backdrop, he framed the discussion around the adequacy of existing legal frameworks, particularly the GDPR, and whether additional protections may be required for intimate AI conversations.

Panellists' contributions

Declan McDowell-Naylor, Information Commissioner's Office (ICO)

Declan McDowell-Naylor argued that the fundamental principles of data protection law remain applicable to generative AI systems and that the GDPR already covers the AI lifecycle, including training and deployment. He noted that chatbot interactions may involve the disclosure of sensitive personal data and observed that many users, particularly younger users, may misunderstand how their information is processed. He highlighted ongoing engagement by the ICO with major AI developers, including regulatory guidance and initiatives such as the children's sandbox programme. McDowell-Naylor emphasised the importance of transparency around personalisation, advertising, and profiling practices, particularly as long-term interactions may generate detailed user profiles. He concluded that users must be given clear information about how chatbot conversations are used and retained.

Yann Padova, Wilson Sonsini Goodrich & Rosati

Yann Padova emphasised that the technology-neutral approach of GDPR remains one of its strengths in addressing rapidly evolving technologies. From a user perspective, he identified transparency and awareness as central challenges, arguing that privacy information is often poorly understood or lost in translation. From the perspective of companies, he highlighted accountability obligations, particularly when processing sensitive personal data. Padova stressed the importance of proportionality throughout the AI lifecycle, including training activities and requests for access to chatbot logs. He also argued that organisations should move beyond privacy-by-design alone and adopt broader security-by-design approaches to protect users' information.

Natascha Gerlach, CIPL

Natascha Gerlach discussed the treatment of chatbot conversations in litigation and discovery proceedings. She argued that existing discovery doctrines are generally technology-neutral and focus on relevance, proportionality, and whether organisations have custody or control over the requested data. However, she noted that chatbot conversations may differ from ordinary business records because many users treat them as quasi-confidential communications that are never intended for public disclosure. Gerlach emphasised that requests for chatbot logs should therefore be assessed through proportionality tests that balance evidentiary value against privacy interests. She also noted that these questions are not unique to U.S. companies and arise across jurisdictions.

Peter Swire, Georgia Tech

Peter Swire focused on questions of discovery, confidentiality and legal protections for chatbot conversations. Drawing on examples from U.S. litigation involving generative AI systems, he discussed the role of pseudonymisation, anonymisation, and protective orders when large volumes of user data are requested in court proceedings. He questioned whether existing procedural safeguards provide sufficient protection for highly sensitive conversational data and examined the practical limits of protective orders in large-scale litigation. His remarks highlighted the growing tension between evidentiary demands and privacy interests as generative AI systems become more widely used.

Panel Questions

Do existing EU data protection rules adequately protect intimate conversations with generative AI, or do we need a new legal regime?

The panel generally agreed that the GDPR provides a strong legal foundation for protecting chatbot conversations. Speakers emphasised that the regulation applies throughout the AI lifecycle and already contains principles relating to transparency, accountability, purpose limitation, and the processing of sensitive personal data. At the same time, several speakers noted that the intimate nature of chatbot interactions creates novel practical challenges, particularly regarding user expectations of confidentiality, long-term profiling, and secondary uses of conversational data.

How can industry players realistically act as "guardians" of user privacy when their business models and technical improvements sometimes rely on accessing and training upon those very conversations?

Transparency emerged as a recurring theme throughout the discussion. Several speakers pointed to the need for clearer explanations of how chatbot conversations are used, particularly in relation to training, personalisation, profiling, and advertising. Attention was also drawn to accountability obligations when sensitive personal data is involved. The conversation highlighted the importance of governance measures that ensure users understand how their information is processed and retained over time.

If a user's chatbot history is requested in civil or criminal discovery, should courts treat these logs as standard electronic evidence or apply heightened protections?

The panel suggested that chatbot logs raise distinct concerns because users often engage with these systems in ways that resemble confidential or intimate communications. Gerlach argued that existing discovery rules should continue to apply but that proportionality assessments must take account of privacy interests and the sensitive nature of many interactions. Swire noted that current legal privilege doctrines generally do not extend to chatbot conversations and cautioned that users should not assume equivalent protections. Several speakers highlighted the growing tension between evidentiary demands and expectations of confidentiality.

Is strong privacy-by-design a potential answer to such concerns?

Privacy-by-design was discussed as an important safeguard but not a complete solution. Speakers repeatedly returned to the need for broader organisational and technical measures, including accountability mechanisms, security protections, and clear user disclosures. Security-by-design was highlighted alongside privacy-by-design, particularly given the sensitive nature of many chatbot interactions. The discussion suggested that building trust in generative AI systems will require a combination of legal, technical and governance measures, rather than any single regulatory or technological intervention.

Moderator: Theodore Christakis, AI.REGULATION.COM Chair, MIAI, University Grenoble Alpes - TC

Panellist 1: Declan McDowell-Naylor. Information Commissioner's Office (ICO) - DMN

Panellist 2: Natascha Gerlach, CIPL - NG

Panellist 3: Peter Swire, Georgia Tech - PS

Panellist 4: Yann Padova, Wilson Sonsini Goodrich & Rosati - YP

Rapporteur: Sruthi Vanguri, University of Amsterdam

CPDP 2026
19th international conference
19-22 May ■ Brussels, Belgium
COMPETING VISIONS, SHARED FUTURES

Secondary use of data under the European Health Data Space: some relevant issues

Date: 21 May 2026

Panel Organiser: University of the Basque Country

Moderator's Introduction

Although the European Health Data Space (EHDS) regulation is hailed as a regulatory achievement, a number of challenges remain. EHDS regulation was approved on 11 February 2025 and will apply from 26 March 2027. Chapter IV covering the secondary use of health data will come into effect in March 2029. Therefore, what is currently being discussed is, in essence, a legal framework that is still under construction and several practical difficulties call for attention. This panel focuses on four of them. First is the role of the Commission, which simultaneously has multiple duties: building infrastructure, enforcing rules and setting standards. The second is the issue of access fees and the methodology for setting them. The third is the interoperability standards, which remain to be drafted. And finally, the fourth is the supervisory architecture, in which different bodies operate under distinct jurisdictions and institutional cultures, producing a particularly complex legislative and application landscape.

Panellists' contributions

Owe Langfeldt, European Commission: Introduction into secondary use framework in EHDS

Within the architecture of EHDS, the Commission wears two hats: one regulatory, the other operational. Under the latter the Commission must build the infrastructure, establish the EU Health Data Access Service for the access bodies of the Member States, and create both the EHDS Board and the Stakeholder Forum, all of which must be in place by March 2027. The Commission is, in addition, charged with adopting implementing acts that will serve as blueprints for subsequent national implementations, to ensure operational readiness by 2029. Applications for the Stakeholder Forum are open, but the members of the Board will be designated by the Member States themselves. When it comes to the infrastructure of EHDS for secondary use, EU

Health Data Access Service will operate as the channel through which researchers submit requests, which are then processed by the relevant national Health Data Access Body (HDAB), with secure processing environments offered as a service. Fees may be required in connection with applications and data requests, intended to compensate the HDAB for the work involved in extracting the data.

Federica Casarosa, Sant'Anna School of Advanced Studies: **The Interplay between technical and legal requirements in the secondary use of health data**

The European Commission has established a centralised infrastructure for data sharing, in which a centralised service at EU level is connected to the national nodes constituted by the HDABs. The legislator has accordingly laid down legal requirements that must be translated into technical ones. A central question is how to access data without necessarily transferring it, an objective pursued through the secure processing environment, a notion already anchored in Article 2(20) of the Data Governance Act. Data reuse is not a one-off arrangement but rather a process composed of a series of steps and functions. Secure processing environment serves as a legally enforceable gatekeeper. There are several open issues still. The first concerns who is going to technically operate the secure environments. This task falls in principle to the national HDABs, yet the requirements imposed on Member States in terms of technical expertise and organisational capacity are demanding. Furthermore, the arrangement carries a risk of institutional self-review as well as a lack of transparency. A second issue arises where the Secure processing environment is set up by a private party. While the national HDAB retains material control over the infrastructure, design choices and incident response remain with the private operator, generating a risk of diluted responsibility and a form of normative delegation through technology. Private actors in such situation effectively translate legal norms into code within proprietary systems and thereby reduce transparency.

Francesca Tassinari, University of the Basque Country: **What role will the standards play in EHDS sharing? – Issues of standardisation**

A key preliminary distinction was drawn between standardisation and interoperability. Standardisation means an adherence to procedures or product specifications. Interoperability, by contrast, is the capacity of two or more systems to exchange information and to make mutual use of the exchanged information. A further distinction was drawn between semantic interoperability and syntactic interoperability, which concerns the meaningful transfer of data between systems. The speaker also outlined the differences between ISO and EU standardisation. An eHealth Network is already in place for the primary use of health data, established under Directive 2011/24 and developed through Recommendation 2019/243. With the entry into force of the EHDS Regulation, this framework becomes mandatory by virtue of Article 14, while Article 15 of the Recommendation 2019/243 supplies the relevant technical specifications (European EHR Exchange Format). For secondary use, by contrast, no comparable infrastructure yet exists and must be created based on the EHDS Regulation. The formal requirements are demanding, and the scope of the concerned data categories is broad, giving rise to a harmonisation gap, since many of the datasets in question are not harmonised at all and will be difficult to harmonise. This gap is to be addressed through the Commission's

implementing acts. Overall, the procedure for standardisation remains highly complex and difficult.

Anastasiya Kiseleva, Vrije Universiteit Brussel: **How to ensure that supervision is not repetitive and contradictory with so many bodies involved in the case of AI medical devices?**

The risk of overlapping and even conflicting supervisory actions is real. By way of illustration, the speaker examined a hypothetical case of an AI company seeking secondary use of health data for development of an AI application intended as a medical device. In such a case the company may at maximum directly or indirectly encounter twelve supervisory bodies, although in practice, in most cases it will be just four. Although mechanisms for interagency coordination exist in the relevant legislation, in practice they function less than smoothly, due to differences between jurisdictions and varying levels of enforcement. Two ways for improvement were proposed. The first consists in streamlining compliance at the operational level by relying on standards capable of demonstrating compliance, while at the same time showing how conformity with one legal framework supports conformity with another. The second operates at a higher level, through the elaboration of standards, guidelines and recommendations designed to assist the supervisory bodies in understanding the interconnections between the various legal requirements and frameworks.

Summary of Q&A discussion

Question 1 (Pablo Trigo Kramcsák, Vrije Universiteit Brussels): We have to have balance between fees and access, especially in the case of smaller researchers. How to balance it?

Answers:

Owe Langfeldt: The problem is "who is going to pay for it". There are rules for the fees, which must be fair, there are some maximums, but otherwise it can be flexible. For example, for academia, the fees can be lower than for business. The Commission will prepare an implementing act that will set the details.

Question 2 (Pablo Trigo Kramcsák): When it comes to international data transfers and requests, can you see any bottlenecks that would make it problematic?

Answers:

Federica Casarosa: One problem might be a different security level of secure processing environments in sending and receiving countries. Another problem might be computational capacity of secure processing environment, for example some might support machine learning, but others would not. What if there is one very good secure processing environment which I want to use, but it is in a different country than the data I need; can I do that? In principle it should be possible, but in reality, it is complication.

Question 3 (Pablo Trigo Kramcsák): What is the role of private standard setters? How will it work in the context of EHDS?

Answers:

Francesca Tassinari: I don't see a direct application of ISO. The adaptation of specific standards in on the EU Commission. We will see in the comitology procedure whether private standard setters will be involved in the preparation of the Commission's implementing acts.

Question 4 (Pablo Trigo Kramcsák): We have the buzzword of coordination. But in practice, what do you think we should do to achieve this aim?

Answers:

Anastasiya Kiseleva: The issue is about coordination of requirements present in the AI Act for the context of medical devices. The manufacturers were prepared to do it even before the AI Act, and they were using AI in medical devices before the AI Act according to the standards for medical devices. But now we are setting new standards, which may be a bit different from the previous ones. And the relevant bodies are not ready to assess the compliance. How to make the coordination? There is a suggestion to exempt manufacturers of medical devices from AI act, but that is not coordination. However, the solution should be that when setting standards, the legislator should take into account other industries and existing legal requirements.

Question 5 (from the audience): How is it with the access to data in the context of AI training? Because in this context, the data will not stay in the safe environment. Will it work?

Answers:

Federica Casarosa: I don't know. The core principle of secondary use in EHDS is to foster technological development. This issue is real. But this is a more general problem of proper anonymisation and pseudonymisation. And in the context of AI learning, we do not have a sufficiently safe environment, yet.

Question 6 (from the audience): What is the interaction between EHDS and EOSC? Is there any?

Answers:

Owe Langfeldt: We are aware of the importance of EOSC, and we are trying to address this issue in the future.

Question 7 (from the audience): Isn't the biggest challenge opt-out of patients?

Answers:

Owe Langfeldt: That is what the legislator decided, and we have to play with that.

Panel Questions

What exactly is the role of the European Commission in the secondary use of data? And how will it be organised?

The European Commission's role within the EHDS is complex. It fulfils several roles simultaneously. First, it acts as a regulator, setting standards and rules through implementing acts that will serve as blueprints for national implementation. Furthermore, it serves as the organisational coordinator for the EHDS Board and the Stakeholder Forum. Finally, it is also the

body responsible for establishing the necessary infrastructure at the EU level through which access for the secondary use of health data will be implemented.

How will access fees be determined? How will the preservation of intellectual property be determined? Could there be forum shopping?

The fees are set to be fair and to realistically cover the costs incurred in enabling the secondary use of health data. The legislation sets maximum limits, but beyond that, the fees can be flexible. For example, they may be lower for the academic sector. Details will be set out in the Commission's implementing act. Forum shopping is theoretically possible but will be difficult to carry out in practice due to the varying technical levels of different HDABs.

What role will standards play in the EHDS?

Standardisation is essential to the proper functioning of the EHDS, as without effective standardisation, it will not be possible to achieve interoperability across the EU. With regard to primary data use, standards based on previous legislation already exist, and the EHDS Regulation merely makes them legally binding. Regarding secondary data use, it will be necessary to develop new standards.

How are we going to ensure that supervision is not repetitive and contradictory with so many bodies involved in the case of AI medical devices?

The main problem is the overlap between regulatory instruments and the various competent authorities. The key to effectively enforcing obligations without creating an unnecessary burden lies in leveraging the synergy of compliance tools that effectively reinforce one another. It is therefore possible to demonstrate compliance under one legal regime by demonstrating compliance under another. This applies both to regulated entities, which should be guided toward such interlinking, and to regulators, who should develop standards and recommendations in a way that allows for such synergies while also respecting existing industry standards.

Moderator: Pablo Trigo Kramcsák, Vrije Universiteit Brussels (VUB) - PTK

Panellist 1: Francesca Tassinari, University of the Basque Country - FT

Panellist 2: Federica Casarosa, Sant'Anna School of Advanced Studies, - FC

Panellist 3: Anastasiya Kiseleva, Vrije Universiteit Brussel - AK

Panellist 4: Owe Langfeldt, European Commission - OL

Rapporteur: Jakub Míšek, Masaryk University / VUB

CPDP 2026
19th international conference
19-22 May ■ Brussels, Belgium
COMPETING VISIONS, SHARED FUTURES

Unpacking the real world impact of the Digital & AI Omnibus - what's at stake and who benefits?

Date: 21 May 2026

Panel Organiser: Ada Lovelace Institute

Moderator's Introduction

The Omnibus proposals had already been the subject of discussion in earlier sessions, and the present panel is dedicated more specifically to exploring how the proposals interact with other instruments of EU legislation. The panel focuses on three levels of interactions: 1) people and society; 2) business; and 3) sovereignty and the role of the EU in the world. The current EU legal landscape consists of a range of new digital legislative instruments designed to support the reusability of data, alongside the regulation of AI. The Union's objective of fostering growth and competitiveness is not new having already be subject of debates surrounding Big Data in 2012. Simplification can prove useful, but only if carried out properly. There is a clear line between simplification and deregulation, and certain elements cannot be simplified without sacrificing the very outcomes they were designed to achieve.

Panellists' contributions

This session took the form of a discussion featuring targeted questions and brief answers. For this reason, the report is structured more like an interview.

Valentina Pavel, Ada Lovelace Institute: Can you walk us through the problem diagnosis on the side of European Commission? How are the goals that are to be achieved with the proposals be measured in the future? Will it be by economic markers, or there will be a specific methodology to measure it?

Karolina Mojzesowicz, European Commission: As part of the GDPR review, the Commission gathered substantial evidence, which was published in its communication of July 2024. Two issues stood out. First was the fragmentation at national level, with the resulting lack of legal certainty. Second was the fact that data protection authorities do not consistently apply the risk-

based approach foreseen by the GDPR. In preparing the Omnibus, the Commission held stakeholder discussions in July 2025, where the general response was supportive of the underlying ideas but critical of the same recurring problems, like fragmentation, legal uncertainty, and an insufficient embrace of the risk-based approach. A further problem is that data sharing simply does not work as intended. Specific contexts, such as cross-border research projects, make the broader difficulties particularly visible, although they remain hard to measure. When evaluating the legal instruments, the Commission focuses on economic effects. Therefore, legal certainty itself will be assessed largely through reductions in compliance costs.

Valentina Pavel: How small businesses see compliance costs and legal uncertainty? Second question aims to the novelisation of Data Act. What do we need to know about the new Data Act when thinking about how it will help the industry (in relation to AI)?

Laura Brodahl, Wilson Sonsini Goodrich & Rosati: The key question is whether the proposals will deliver the real impact they ought to have, and in particular whether they will genuinely achieve simplification. Simplification is not deregulation. A good example of meaningful simplification would be the centralisation of incident reporting on a single platform, with distribution to the relevant authorities handled in the backend. At first glance, merging several pieces of legislation into one might look like simplification, but in practice it produces little real effect. What truly needs simplification is enforcement. Both companies and authorities need to understand clearly who is responsible for what. The law, however, leaves considerable leeway to the Member States, and different authorities come into play depending on the type of data involved, so the underlying fragmentation persists.

Valentina Pavel: What sort of impact can you see in the Omnibus proposals?

Max von Thun, Open Markets Institute: The question of why this is happening now is relevant. It seems that GDPR has, to some extent, been turned into a scapegoat for Europe's broader failure to succeed in the digital economy. A good deal of what the Omnibus proposes is genuinely sensible. The centralisation of incident reporting and the rationalisation of cookie rules are clear examples. Many of the proposed changes, however, do not actually deliver simplification and are problematic from a fundamental rights perspective. Part of the difficulty is that they apply to all companies, including the largest ones. Rather than supporting EU competitiveness the proposal also helps the big tech companies. Examples include the scaling back of data subject rights such as access and information rights, the redefinition of personal data, and the loosening of conditions for processing in the context of AI training. A recent report indicates that many of these changes would, in fact, help US tech giants to avoid GDPR enforcement. EU companies may well benefit, but the big tech players stand to gain considerably more, since they already enjoy a competitive advantage on which they can readily build.

Karolina Mojzesowicz: Responded defensively to the allegation that the proposals favour big tech. The proposed exemptions are in fact designed to help small businesses. As for the right to information about personal data processing, the standard would not be lowered, since the proposed change is aimed at addressing abuse of the right rather than curtailing it. The exchange sparked a heated discussion among the panellists.

Valentina Pavel: What is clearly at stake for the people and society when it comes to these proposals and their connection to other legislation? What will be the impact?

Orla Lynskey, UCL Faculty of Laws: Fragmentation within the internal market is profoundly problematic and must be addressed, although simplification need not slide into deregulation. The Omnibus proposal is essentially a recalibration exercise that shifts the balances of data protection law in favour of ongoing data processing. As the ongoing debate on the redefinition of the right of access already illustrates, this is not really simplification. Some elements of the proposal are particularly troubling, the redefinition of personal data being foremost among them. Such changes should not be pushed through in emergency mode but rather pursued properly, with all relevant stakeholders involved. Two examples were offered. First, under the AI Act, minimal risk AI systems are now required to register, but this obligation is set to disappear. That is problematic, since the registration at least made it possible to see which companies had self-assessed as minimal risk and to review those assessments. Second, the proposed change to the right of access effectively shifts the burden of proof. The controller could now claim that a request does not concern realisation of personal data rights and refuse to give access, leaving it to the data subject to prove that they are in fact entitled to it.

Valentina Pavel: Walk us through specific provisions of Omnibus and show us how these changes aim to achieve EU Commission's strategic objectives.

Karolina Mojzesowicz: In the context of GDPR, the proposed changes will deliver simplification through clarification and thereby reduce compliance costs. The redefinition of personal data is, in her view, nothing genuinely new, since the issue has been with us at least since CJEU Breyer Case (C-582/14). She set her argument in a very strong subjective (relative) approach to personal data definition and claims that the case law of CJEU is entirely in line with this approach and that it had always been so. Making legitimate interest easier to rely on in the AI context likewise cuts compliance costs, as does the clearer framing of research exception. Lower compliance costs under the GDPR will, in turn, have a positive spillover effect across all other instruments that rely on it.

Valentina Pavel: What is your perspective on the strengthening competitiveness by Omnibuses?

Laura Brodahl: The proposal creates new ways to access data and that is good as a general goal. However, the data in question are legally protected for very good reasons and we have to find proper balance between conflicting rights. That is hard and the law should help with that.

Valentina Pavel: Who captures the economic value of data processing and AI? Who benefits from it?

Max von Thun: Given the way the market is currently structured, the principal beneficiaries will, at this moment, be the big tech companies, as they already enjoy a range of significant advantages such as data, platforms, services and infrastructure. Genuine innovation, moreover, cannot be expected when investment in infrastructure remains so limited. Without functioning infrastructure, it simply will not happen. More broadly, the concern is that the various exemptions introduced by the Omnibus reform will, in the present circumstances, mostly benefit those who already enjoy substantial advantages.

Valentina Pavel: What scenarios do you see and how to counterbalance it?

Orla Lynskey: We have to ask what society actually gains if one set of contested rules is simply exchanged for another set of equally contested ones. The Omnibus proposal brings a shift in balances rather than a genuine improvement and simplification. The example of legitimate interest as a basis for AI learning is a case in point. It fails to take existing case law properly into account, while at the same time still leaving open the possibility of relying on consent. That is an outcome that does little to remove fragmentation.

Laura Brodahl: Maybe we should not create new rules but support the infrastructure.

Karolina Mojzesowicz: There are existing frameworks for infrastructure support.

Laura Brodahl: Yes, but they did not catch up properly to effectively create new opportunities for new infrastructure to be built.

Summary of Q&A discussion

At the end of the discussion, a large number of questions were collected at the same time, but unfortunately, they could not be answered in detail due to time constraints and the need to make way for the next panel.

Question 1 (From the audience): What type of innovation do you expecting to achieve from this reform?

Answers:

Max von Thun: We should be able to say what kind of innovation do we want to have in the Europe.

Question 2 (From the audience): Would we have this discussion if there was someone else in the government at the other side of the Atlantic?

No answer was provided.

Question 3 (From the audience): I want to ask about the definition of personal data and the real outcomes of the definition. For example, there is a practical problem with joint controllership? In other words, did you think it through to the practical outcomes?

Answers:

Orla Lynskey: These practical problems arising from the definition of personal data were solved and can be solved through interpretation and work of DPAs and Courts. There is no need to redefine it in the law.

Question 4 (From the audience): Does the wording of research exception mean that the large AI companies can use it?

Answers:

Max von Thun: Yes, I have the same fear.

Orla Lynskey: I expect this to be clarified in the following legislative process.

Question 5 (From the audience): AI and prohibition of sexualised deep fakes. There is too much focus on the outcome, but there can be much harm even without picturing genitals. The rules can be interpreted that it allows web scraping of pornography for AI. Why was the proposal prepared in the way that it benefits the big companies? Why was the civil society left out?

Answers:

Karolina Mojzesowicz: We engaged with the civil society very deeply.

Panel Questions

When analysed together, what will the cumulative effect of the proposed omnibus changes on people's rights and protections and on European businesses be?

There was no consensus on this issue during the panel discussion. The representative of the European Commission insisted that there would be no lowering of the standard of personal data protection, as the changes merely entail technical clarifications of obligations that will lead to greater legal certainty and thus reduce costs for the business sector. The remaining speakers were quite sceptical about this issue. In particular, the redefinition of the term "personal data" and the restriction of the right of access to data were identified as problematic aspects of the proposal. The omnibus proposal was described as a shift in the balance between the interests of data controllers and data subjects towards the controllers.

Will the proposals achieve the Commission's various digital strategies in practice?

The panelists did not reach a consensus on this issue. The goal of these legislative efforts is to improve the EU's competitiveness in the areas of data utilisation, digital technologies, and AI. The Commission approaches this issue from an economic perspective and argues that if simplification leads to a reduction in compliance costs, this will also contribute to achieving these goals. Critics, however, point out that the proposal contains a large number of changes that do not lead to simplification but rather constitute deregulation. As such, they lower the level of protection of fundamental rights and are undesirable. At the same time, the proposal lacks elements that could actually help the situation, such as support for the construction of necessary infrastructure.

In what ways do these changes support — or undermine — a value-driven European vision for a competitive, secure, and rights-based digital economy?

Simplifying regulations, whether in the context of the GDPR or data and AI regulation, is an essential process that will genuinely lead to greater legal certainty, lower costs, and, ultimately, benefits for consumers. However, this must not amount to deregulation, as is often the case with the Digital Omnibus proposal. As it seems, at the moment, the result is a lowering of the standard of protection for fundamental rights, and there is no guarantee that the EU's digital industry will actually be supported.

What are the implications for Europe's sovereignty and its position as a normative power in global digital governance?

A badly designed regulation that leads to deregulation rather than simplification cannot help European digital businesses, such as innovative startups and other small and medium-sized enterprises. The problem is that the exemptions being introduced will benefit global big tech companies the most, as they have a competitive advantage in the form of existing data, services, and infrastructure. Without targeted support for European companies to address this gap, the legislative changes alone will not be sufficient.

Moderator: Valentina Pavel, Ada Lovelace Institute, VP

Panellist 1: Karolina Mojzesowicz, European Commission, KM

Panellist 2: Max von Thun, Open Markets Institute, MT

Panellist 3: Orla Lynskey, UCL Faculty of Laws, OL

Panellist 4: Laura Brodahl, Wilson Sonsini Goodrich & Rosati, LB

Rapporteur: Jakub Míšek, Masaryk University / VUB

CPDP 2026
19th international conference

19-22 May ▪ Brussels, Belgium
COMPETING VISIONS, SHARED FUTURES

After the Omnibus: Consent or Red Lights?

Date: 21 May 2026

Panel Organiser: Ping (Privacy in Germany) & German Bar Association (Deutscher Anwaltverein)

Moderator's Introduction

Niko Härting, Ping (Privacy in Germany) & German Bar Association, started the panel by welcoming the attendees and thanking the panel's sponsors. He highlighted that in October/November last year, there was a lot of discussion in Germany about the potential reform to GDPR, well before the Omnibus package. In this respect, the panel will be focused on the former discussion rather than on the Omnibus, particularly on consent after the CJUE judgments limiting what can be done with other legal basis.

Panellists' contributions

Merel Van Aar, Fieldfisher

Merel Van Aar began by highlighting that her work advising non-EU companies in data-related topics involved addressing the role of consent. In particular, she stressed out that her practice usually revolved around trying to find ways to move out of consent towards other legal basis. Turning specifically into her reflections about GDPR's role, she pointed that the GDPR is, after all, an internal market instrument, beyond its capabilities to protect fundamental rights. This, for example, becomes a critical theme in certain domains, such as healthcare, where Member Sates have specific legislation that can hinder the uniform approach provided by GDPR, for example in the case of clinic trials, which demand assessing each involved Member State legislation to meet their consent standard.

Christopher Millard, Queen Mary University of London

Christopher Millard opened his presentation by asking how did consent become so popular in Europe, particularly taking into account its residual origins in Convention 108 and the fact that all legal basis stand on an equal footing. He attributes this to two phenomena. Firstly, the change in Convention 108+ with regards to the role of consent. And secondly, to the imported practices from US companies that rely on consent. In this latter scenario, he argued that the US relies on

consent because it is the only political common ground between parties, as for democrats it is better than noting and for republicans it embodies the libertarian spirit.

Christiane Wendehorst, University of Vienna

Christiane Wendehorst focused her presentation on the concerns she has over the reliance on consent and current practices. In this sense, she mentioned that, as part of her work at the European Law Institute, there is something to be gained from the US approach, particularly from their uniform legislation practices. In this sense, the US model law for data protection from 2021 put forward a traffic light approach for data processing activities, with 'red' activities being incompatible without having collected consent from users. While this was a legislative failure in the US, the approach would be interesting to be taken for any discussion in the EU about reforming GDPR. In particular, she highlighted that the EU has already adopted traffic light-like schemes in other pieces of digital legislation, such as the AI Act.

Markus Wünschelbaum, Data Protection Authority Hamburg

Markus Wünschelbaum started by explaining what he is doing as part of his job of Digital Data Strategist, which involved doing foresight work for all German DPAs. In this respect, he is hesitant about the actual success of the Digital Omnibus, as it lacks its impact assessments, which may or may not happen until 2027, pushing the whole package to, at least, 2029. In this sense, he believes that GDPR reform, through other political and legislative processes could be a more realistic path to be pursued; ultimately, he believes that these attempts will not come to fruition and we will have to address consent and its problem under the existing frameworks. After Markus Wünschelbaum presentation, Christiane Wendehorst took the microphone again and agree that analysis but warns about success change from politicians, putting as an example the situation with the sale of goods legal rules in the EU.

After this general round of presentations, Niko Härting posed a question to spark discussion in the panellist about why there are no prohibited practices when it comes to data processing and whether consent can be used enable horrible (sic) practices. In this respect, Merel Van Aar argued that the balancing between fundamental rights protection and enabling economic practices should dominate any consent-collection deployment activity. Christiane Wendehorst stated that her proposed traffic lights approach could already be deployed in existing legislation through the fairness principle in GDPR but also through the UCTD. Christopher Millard agreed with Christiane Wendehorst about the role of fairness, with Markus Wünschelbaum stating that this is a data protection by design mechanism that is often overlooked. In this respect, Markus Wünschelbaum called for also look for other 'red lights' outside of GDPR to support this approach. Following this, Christopher Millard argued that there are also 'green lights' for certain activities that are required by law.

The panel, mainly with interventions from Christopher Millard, Merel Van Aar and Markus Wünschelbaum, then turned to criticise the fixation on consent and the lack of awareness about the role that other legal basis can play in the configuration of data processing activities. Moreover, these panellists also highlighted that if the intention of the EU is to put users at the centre, this can be done with other data protection mechanism such as the right to object or the right to data portability rather than having consent as the legal basis to enable a processing activity in the first

place, as noted particularly by Merel Van Aar who called this a true alternative to the US approach based around consent.

On a closing note, Christopher Millard argued that consent, in its current configuration, is ill prepared for an AI agents era where consent is not granted by the user but rather through an AI proxy, calling for caution in finding ways to make this scalable.

Summary of Q&A discussion

The first question focused on the European Health Data Space and the role of consent as an opt-out mechanism rather than a proper legal basis to support data processing. Markus Wünschelbaum says the this approach is a result from consent fatigue and forcing a switch towards other legal basis to achieve bigger objectives, such as health research. Christopher Millard says that while this data space made this design decision there are other mechanism that still preserve consent in this context, such as the data altruism in the DGA.

The second question revolved around the Digital Omnibus and the impact assessments; this was tackled by Markus Wünschelbaum arguing that their lack is concerning and should be addressed as soon as possible. Christopher Millard also tackled the manner by arguing that there is a lot going on and when the political decision is taken we are going to find ourselves in a situation that nobody wanted to arrive to.

A final question revolved around the connection between a processing activity being fair when based on question. The panel argued, in an almost joking manner, that it depends on the situation, given the lack of time to properly address the question and to avoid giving a shallow answer.

Panel Questions

In which cases is consent appropriate to protect personal data?

Consent is most appropriate in contexts where a genuine, informed choice can be meaningfully exercised by the individual, though the panel underscored that consent was never intended to be the primary legal basis under GDPR, as all legal grounds stand on equal footing. Its current dominance is attributed to two exogenous factors: the revision of Convention 108+ and the importation of US commercial practices, where consent became the only viable political compromise between liberal and libertarian sensibilities. The panel signalled that consent remains relevant in highly sensitive domains such as clinical trials, where each EU Member State imposes its own specific consent standards that practitioners must individually assess. However, even in these cases the adequacy of consent as the operative mechanism is contested, particularly as it proves structurally ill-suited for emerging contexts such as AI agents, where consent would no longer be granted by the user directly but routed through an automated proxy.

And in which cases would it be useful to define red or green lines that distinguish between illegal and lawful processing without leaving it up to the individual data subject to protect their own data?

The panel converged on the view that a traffic-light framework for data processing activities would be a productive structural alternative to consent-centric regulation, with 'red' activities designating those that are categorically impermissible without prior user consent and 'green' activities marking those that are affirmatively required or authorised by law. This approach was drawn from the 2021 US model law for data protection, which, despite failing legislatively, offered a conceptual template that the panel found transferable to EU reform discussions. Crucially, the panel noted that the EU has already implemented analogous tiered schemes in other digital legislation, most notably the AI Act, which suggests the traffic-light logic is not foreign to the Union's regulatory toolkit. Beyond GDPR itself, the fairness principle within GDPR and the Unfair Contract Terms Directive were identified as existing legal anchors through which red-light categories could already be operationalised, and supplementary red-light constraints available outside GDPR were also flagged as an under-explored resource.

How can we balance the need for informed consent with the practical realities of user experience, especially when consent banners are often seen as a formality?

The panel diagnosed the consent banner phenomenon as symptomatic of a structural misplacement of consent as the dominant legal basis, rather than as a failure of implementation alone. The discussion pointed to consent fatigue as a documented driver of design choices already visible in EU legislation, citing the European Health Data Space's adoption of an opt-out mechanism in lieu of proper consent-based processing as a concrete institutional response to this problem. Rather than attempting to rehabilitate consent UX, the panel argued that genuinely placing users at the centre of data governance is better achieved through alternative mechanisms, specifically the right to object and the right to data portability, which operate downstream of the legal basis determination and do not burden users with gatekeeping decisions at the point of data collection. This reorientation was explicitly described as a 'true alternative to the US approach' centred on consent and was presented as more aligned with the internal market logic that fundamentally animates GDPR.

What role should regulators/lawmakers play in setting boundaries for consent and its alternatives?

The panel held that regulators and legislators bear primary responsibility for defining the categorical boundaries of lawful and unlawful processing, rather than delegating that determination to individual data subjects through the consent mechanism. DPAs were identified as having an underutilised instrument in data protection by design, with the fairness principle serving as an available but frequently overlooked regulatory lever for drawing substantive lines around processing activities. On the legislative side, the panel expressed considerable scepticism about the Digital Omnibus as a near-term reform vehicle, noting the absence of impact assessments and projecting that the package would likely not produce operative changes before 2029, making reform through other political and legislative channels a more realistic path. Ultimately, the panel's prevailing assessment was that consent's structural problems will need to be addressed under the existing legal framework, placing the interpretive and enforcement responsibilities squarely on regulators applying tools such as the GDPR fairness principle, the UCTD, and design-based obligations that do not wait for legislative intervention.

Moderator: Niko Härting, Ping (Privacy in Germany) & German Bar Association - NH

Panellist 1: Christiane Wendehorst, University of Vienna - CW

Panellist 2: Christopher Millard, Queen Mary University of London – CM

Panellist 3: Markus Wünschelbaum, Data Protection Authority Hamburg - MW

Panellist 4: Merel Van Aar, Fieldfisher - MA

Rapporteur: Andrés Chomczyk PenedO, Universidad Pontificia Comillas/Vrije Universiteit Brussel

CPDP 2026
19th international conference
19-22 May ■ Brussels, Belgium
COMPETING VISIONS, SHARED FUTURES

Rhetoric over rights: the Digital Omnibus, competitiveness and the end of European values?

Date: 21 May 2026

Panel Organiser: Unabhängiges Landeszentrum für Datenschutz (ULD)

Moderator's Introduction

Felix Bieker opened by noting that this was one of several CPDP panels on the Digital Omnibus. He proposed framing the discussion around rhetoric rather than the Omnibus's specific provisions. The Draghi report, he argued, had influenced the Commission. After a decade spent building a data-protection framework, it was now hitting the brakes in the name of innovation and of competing with the United States and China on AI on their terms, with European values demoted in both rhetoric and substance. He read this as an old ideology of deregulation and of empowering large business and observed that the harms of AI-driven decision-making fall first on marginalised groups, who become its testing ground, not only in the United States but also in the Netherlands, in Danish social services and in German policing. None of these problems are new, researchers, civil society, and affected communities have been sounding the alarm for years. He cautioned that simplification and efficiency also serve to remove democratic checks and balances, and that the Commission has been dismissive of researchers and of foundational critique.

Panellists' contributions

Across the panel, the shared call was for evidence over rhetoric and for enforcement over the reopening of hard-won law.

Maria Magierska, University of Maastricht

Magierska welcomed the framing around rhetoric, arguing that the debate turns on big words, like simplification, deregulation, competitiveness, innovation, digital sovereignty, invoked without any shared sense of what they mean. She accepted that US firms process far more data than their European counterparts but disputed that simplification is the only route to competitiveness or

digital sovereignty. Only parts of the Omnibus, she said, are genuine simplification; the changes to the definition of personal data and to legitimate interest go further, reopening the GDPR itself. Europe's distinguishing strength has been precisely its rules, so stripping them removes what sets the Union apart.

Itxaso Domínguez de Olazábal, EDRi

Domínguez de Olazábal, from academia and civil society, noted several omnibus packages in key areas are on the table at once. The Commission's message is that they must pass them quickly, and bundling disparate amendments leaves Parliament and Council feeling bound, with a lack of impact assessments to the fundamental-rights stakes. The real priority, she argued, should be enforcement and the protection of people, not handing companies more power to self-assess fundamental rights. Competitiveness should not mean shielding the largest players, in her view big players like Google should be broken up, not protected. She questioned the evidence base of the Draghi report, pointing out that she has taken part in the consultations and that the headline figures remain unexplained even as the Commission repeats them. She pointed to a lobbying asymmetry in which industry vastly out-resources civil society, scores of companies are visible in the Parliament's transparency register. A particular danger of the digital Omnibus, she warned, is companies simply self-asserting that the GDPR does not apply to them, a stance then propagated down supply chains.

Midas Nouwens, Autoriteit Persoonsgegevens

Nouwens gave the regulator's perspective. The Dutch DPA's official position is that it supports simplification provided fundamental rights are protected, but the EDPB opinion is quite critical. The legislative proposals lack effective impact assessments and contain inconsistencies and confusing terminology between articles and recitals, so their drafting quality is poor. The compressed timeline consumed scarce DPA resources and crowded out other work, for instance the effort to issue guidance on whether generative AI can be lawfully developed and deployed. How found it puzzling that a new AI-specific legitimate-interest basis is introduced, although the authority's own (unfinished) analysis suggests the same outcome is already possible under the current GDPR, which raises the question of why it is needed.

Summary of Q&A discussion

Question 1: Concern about the lack of evidence behind these claims.

Answers:

The panel agreed the evidence is largely absent. Itxaso Domínguez de Olazábal noted she has been part of the consultations and that many figures are never explained, Maria Magierska called the 'declare it nonpersonal and free up capacity' logic a gamble with no supporting evidence, Midas Nouwens said meaningful engagement requires evidence and that he is not persuaded that cases reaching the CJEU prove the definition of personal data is ambiguous.

Question 2: How do we keep our principles from the GDPR but make them simpler, since they are difficult to enforce in practice?

Answers:

Maria Magierska suggested that the CJEU plays a big role in how the principles are interpreted and applied, for DPAs, so Courts are key here. Midas Nouwens wonders if the Jered approach of the AI Act and DSA might reduce the interpretative Jme-consuming work DPAs must do. Also referred to listing of prohibited/allowed practices discussed earlier.

Question 3: Competitiveness is a legitimate concern, how to engage with different parliamentary groups about the proposal in earnest?

Answers:

The panel agree there might is a problem with European Competitiveness. Perhaps it is easier to focus on the red tape of regulation as the problem, rather than engage with other solutions. However, friction can be valuable to protect fundamental rights, cybersecurity, and businesses, each of which can be prioritised by different actors. The panel also observed that the real negotiations happen with unequal access behind closed doors, and that engagement must be evidence-based rather than purely oppositional.

Question 4: How do we bridge the gap between businesses and policy makers, in light of the hatred towards platforms that is felt?

Answers:

Felix Bieker pushed back on the word 'hatred' toward platforms, distinguishing sustained criticism of platform practices from animus toward business. Maria Magierska and Itxaso Domínguez de Olazábal saw that there was no lack of issue with big companies getting access to policymakers as discussed earlier. Itxaso Domínguez de Olazábal warned against scapegoating a single platform when addictive design is internet-wide and called for a level playing field in which all are scrutinised.

Panel Questions

How can we resist and change the current narrative in academia, activism and practice?

The panel saw distinct but complementary roles. Academics, especially in law, should abandon the pretence of objectivity and acknowledge their standpoint. Furthermore, they should teach critical thinking, equipping (often private sector) practitioners to question rather than recite rules. Civil society has been ignored, because of the activist label, however, they have knowledge and should be taken seriously. Furthermore, they should try to build bridges across movements, as the issues are intersectional, and counter an asymmetry in which lobbyists are heard over researchers. Data-protection authorities are more constrained, since they must protect their own perceived legitimacy which can be weakened by appearing too strict or only punishing. However, they can still warn the public, share evidence, and resist purely rhetorical claims. A recurring

theme was the need to get ahead, rather than perpetually run behind both the technology and the Commission.

What does the Digital Omnibus reveal about whose rights the EU is willing to weaken, and how do we defend people's rights when competitiveness becomes the overriding political priority?

The speakers pointed to marginalised groups, migrants and children as the first to bear AI driven harms. Weakening the GDPR, weakens rights of everyone as individuals and societally. For example, permitting other legal bases, not only consent, for accessing data on smart phones, cars or devices would deepen tracking without awareness or choice.

They warned that the Omnibus shifts power to companies as self-assessors of fundamental rights, and that the individual is progressively pushed out of enforcement as cases move from the national authority to the EDPB and the courts, leaving little procedural influence. On enforcement, Maria Magierska noted that individual data-subject complaints are currently treated as less worthy of action and are often answered with a leger from DPAs rather than a full investigation. Addressing the issue of different types and volumes of processing, for enforcement, would be valuable in this regard.

Is competitiveness a quality that should be pursued, and can it be achieved only through deregulation or simplification?

The panel accepted that the competitiveness concern is real and US firms hold a data advantage but rejected the claim that deregulation or simplification is the only path to it. Europe's rules were presented as its distinguishing strength, not merely a burden; alternatives raised included breaking up dominant players, single-market choices, and support for open source.

Crucially, the speakers saw no evidence that loosening the definition of personal data would improve competitiveness, calling it a gamble. Indeed, it would make enforcement harder, by adding more grey zones for DPAs who are already struggling in terms of resources and complaints. As a constructive route, Midas Nouwens suggested that more outright forbidden practices, e.g., a black-list or white-list approach seen in other instruments, could deliver both simplification and clearer protection. Maria Magierska also noted that much innovation has historically been publicly rather than market-funded in Europe, so it is unclear whether the Omnibus will address competitiveness. Finally, legal uncertainty is difficult for enforcers and businesses.

Is the Digital Omnibus merely closing the enforcement gap by legalizing current practices?

Several contributions pointed that way. The new AI-specific legitimate-interest basis appears to legalise what may already be possible under the GDPR; enlarging the 'non-personal' space risks bringing non-compliant practices within bounds rather than curbing them; and companies are increasingly self-asserting that the rules do not apply. The panel argued that the genuine fix, i.e., better enforcement, a duty for authorities (e.g., competition authorities and DPAs) to cooperate, adequate resources and expertise, and attention to the CJEU's broad readings of core notions, has been neglected in favour of reopening the substantive law. Midas Nouwens also criticised the Omnibus as solutionistic, reshaping a deliberately technology-neutral GDPR around AI

specifically, with a legitimate-interest provision naming AI, and research framing reminiscent of Facebook's past 'it's research defence' for A/B testing. This approach, she thought was not workable in the long run, since next year the pressure could come from something else, like neurodata instead.

Itxaso Domínguez de Olazábal cautiously applauded one long-demanded gain from civil society in the Omnibus i.e., machine-readable privacy signals. This would let people refuse or allow tracking automatically and have the choice remembered, potentially ending cookie banners on the internet.

Moderator: Felix Bieker, ULD and FIZ Karlsruhe - FB

Panellist 1: Maria Magierska, University of Maastricht - MM

Panellist 2: Itxaso Domínguez de Olazábal, EDRi - IDO

Panellist 3: Midas Nouwens, Autoriteit Persoonsgegevens - MN

Rapporteur: Kimmy Shah, VUB

CPDP 2026
19th international conference
19-22 May ■ Brussels, Belgium
COMPETING VISIONS, SHARED FUTURES

The future of technology is about more than AI: A conversation about right sized technology

Date: 21 May 2026

Panel Organiser: Mozilla Foundation

Moderator's Introduction

Claire Pershan opens the panel by stating that technologies should be people-centred, prioritising communities and supporting their development rather than advancing at their expense. Yet this vision remains far from the dominant technological reality. Today's technology landscape is increasingly concentrated, characterised by expanded data extraction, surveillance, and energy consumption. Meanwhile, it is becoming progressively detached from the communities it should serve. As Europe appears to be at a critical turning point, it is important to reassess whether current technological systems align with societal values and genuinely promote public well-being.

Panellists' contributions

Agnès Crepet, Fairphone, Le Mouton Numerique

Agnès Crepet explains that Fairphone has spent over a decade demonstrating that ethical, repairable, and long-lasting smartphones can be commercially viable. However, a major challenge for small- and medium-sized enterprises like Fairphone is the limited capacity to dedicate resources to lobbying and regulatory engagement. Drawing on the perspective of her small- and medium-sized social enterprise, she makes three key recommendations. Firstly, she advocates for stronger European regulations on ecodesign, repairability, and digital fairness. For example, she highlights ongoing efforts to improve spare-part availability, software support, interoperability, and open-source access. Secondly, she advocates for a decolonial approach to technology development that considers the conditions of workers across global supply chains, as confronting the structural inequalities underpinning technological production is the foundation of solutions to many other problems. Finally, she suggests that policymakers could

promote sustainable technology by requiring public administrations, schools, and government institutions to procure environmentally sustainable and long-lasting products.

Benoît Courty, CodeCarbon

Benoît Courty begins by introducing CodeCarbon, a project which committed to addressing the substantial environmental costs of increasingly large AI models. From his perspective as a data scientist at CodeCarbon, he notes that open-source AI projects are supported by civil society. However, it also means that these projects depend on community participation, ongoing maintenance, and sustainable funding, whereas organisations such as CodeCarbon lack the financial backing typically available to large corporations. He further suggests that fine-tuned, task-specific models may offer comparable performance to large general-purpose systems while requiring significantly fewer resources. Beyond environmental concerns, Benoît Courty emphasises the broader societal implications of AI, including potential job displacement and the risk of humanoid robotics. He therefore points out the need for policymakers to consider transparency regulations, taxation mechanisms, and social welfare measures. Finally, he highlights the importance of customer empowerment.

Nadia Nadesan, Civic Tech/Platoniq

Nadia Nadesan highlights the issues of inequality in AI. She explains how technology companies can exploit social inequalities and precarious forms of labour, reinforcing existing power imbalances through the development and deployment of AI systems. To address these concerns, Nadia Nadesan calls for greater emphasis on public-interest AI. She suggests having smaller, domain-specific systems that are transparent, contestable, and aligned with democratic values. Furthermore, she stresses the importance of accessible mechanisms for redress when AI causes harm and the need to account for the intersecting forms of discrimination that can disproportionately affect marginalised communities. More specifically, she advocates for sustained investment in shared public infrastructure, long-term maintenance, and local expertise, while shifting priorities from short-term optimisation toward resilience, democratic accountability, and international cooperation.

Summary of Q&A discussion

Question 1: The Panoptykon Foundation (Fundacja Panoptykon) participant: To what extent can initiatives promoting responsible AI meaningfully transform current technological trajectories? What role can society play in supporting such efforts?

Answers:

Benoît Courty: Meaningful progress in this area depends largely on effective policymaking, as major technology companies have not consistently aligned with broader societal and public-interest objectives. While some positive developments have been observed, substantial regulatory and institutional efforts remain necessary to address the challenges posed by the current trajectory of technological development.

Agnès Crepet: After more than thirteen years of advocacy, Fairphone continues to grow and has achieved several significant policy successes. Sustained collective action can produce meaningful regulatory change, even when progress appears incremental.

Nadia Nadesan: It is important to identify and engage unconventional allies as digital infrastructure increasingly entangles with environmental and territorial governance, underscoring the need for cross-sectoral coalitions that align technological, ecological, and community interests.

Question 2: A student from the University of Glasgow: In addition to monitoring the environmental impact of data centres, are alternative solutions also being explored in CodeCarbon? To what extent are the origins of spare parts of Fairphone products examined?

Answers:

Benoît Courty: A potential component of the solution involves deploying smaller, locally situated data centres co-located with end-use demand and designed to enable the reuse of waste heat and water resources.

Agnès Crepet: There is limited industrial research and development, constraining progress in this regard. However, while full recovery of raw materials remains highly challenging, partial recovery and component refurbishment are presented as a more feasible and pragmatic approach within existing production cycles.

Question 3: How can policymakers incorporate the ideas discussed in this panel into their decision-making processes when defining technological sovereignty?

Answers:

Agnès Crepet: There is a need to adopt a broader perspective on how the technology sector can be improved globally, particularly in relation to decolonial considerations.

Benoît Courty: A gradual, step-by-step process should be proposed in which greater local control over digital infrastructure (such as hosting and software stacks) is pursued alongside more targeted and strategically oriented public spending.

Nadia Nadesan: Defining sovereignty within cultural heritage data spaces requires establishing reciprocal and non-extractive conditions for data reuse.

Question 4: A member of a startup in Austria: How can innovation be redefined to recognise and support the idea discussed in this panel?

Answers:

Nadia Nadesan: Design with a multi-generational perspective and promote considerations of long-term human and technological stewardship, including what societies choose to preserve and transmit over time.

Agnès Crepet: A key challenge lies in transforming entrenched tech culture. It is difficult to change large technology companies. Therefore, an inherently long-term process that begins with education and socialisation is recommended.

Question 5: In an era of intensifying geopolitical competition between a largely deregulated American technological model and a more centrally governed Chinese model, how should Europe develop a regulatory and policy framework that balances innovation and global competitiveness with its own normative commitments?

Answers:

Benoît Courty: The issue of funding remains a significant challenge due to the scale of capital required.

Agnès Crepet: The concept of 'slow tech,' while potentially perceived as discouraging innovation, reflects established industrial practices such as those in the European automotive sector.

Nadia Nadesan: The dominant narratives of growth and innovation are increasingly being challenged, as exemplified by developments such as DeepSeek, which question assumptions about elite education, high capital requirements, and cutting-edge infrastructure. A genuine innovation arises from critically rethinking entrenched paradigms rather than maintaining a narrow focus on financial success and competitive dominance.

Question 6: How could these ideas move into the mainstream?

Answers:

Agnès Crepet: We can consider the role that public institutions could play in facilitating the mainstream adoption of such technologies.

Nadia Nadesan: Despite perceived incentives toward conformity, articulating one's values and critical perspectives is essential for forming meaningful alliances and driving institutional change.

Panel Questions

How can policymakers incentivize an ecosystem that privileges mission-aligned technologies?

Policymakers can incentivise such an ecosystem by means such as, but not limited to, taxation mechanisms, social welfare measures, and requiring public institutions to choose and procure products that align with their values. However, in addition to these incentives, stronger regulations are still necessary.

How can businesses design products for real communities and not only for market growth?

Businesses should incorporate several important principles into their design. Firstly, take a decolonial approach that aims to minimise global structural inequalities. Secondly, take a multi-generational perspective that considers long-term societal values. Finally, build cross-sectoral and unconventional coalitions that can further contribute to the goal.

How do principles like user choice, agency, interoperability, modularity, and open source contribute to the success of these technologists? What about circularity, right to repair, and ecodesign?

These principles encourage organisations to critically reassess entrenched paradigms rather than to maintain a narrow focus on financial performance and competitive advantage. Such a perspective creates the conditions for genuine innovation by fostering alternative ways of thinking, organising, and creating value beyond conventional market-driven objectives.

How can consumers - how can people - express their preferences for worthy technology, that serves us and that can be sustained over time and within planetary boundaries?

Customer/citizen empowerment is essential, as they provide the fuel for an active civil society capable of driving institutional change. In addition, it is also recommended to transform entrenched technological cultures through long-term processes of education, awareness-building, and socialisation. Given the considerable challenges of reforming large technology corporations directly, fostering change at the societal level may be a more effective and sustainable pathway.

Moderator: Claire Pershan, Mozilla Foundation - CP

Panellist 1: Benoît Courty, CodeCarbon - BC

Panellist 2: Agnès Crepet, Fairphone, Le Mouton Numerique - AC

Panellist 3: Nadia Nadesan, Civic Tech/Platoniq - NN

Rapporteur: Ting-Yu Yu, the University of Edinburgh

CPDP 2026
19th international conference
19-22 May ■ Brussels, Belgium
COMPETING VISIONS, SHARED FUTURES

When Big Tech rules universities: reclaiming academic freedom through digital sovereignty

Date: 21 May 2026

Panel Organiser: AlgoSoc

Moderator's Introduction

Moderator Maria Luisa Stasi opened the discussion by reflecting on academic freedom as a longstanding but fragile principle that requires continuous protection. She noted that academic freedom is not solely about safeguarding the interests of academics, but about preserving the societal benefits that arise from independent research and teaching. The discussion focused on the extent to which growing dependence on digital infrastructures provided by large technology companies may affect the ability of universities to operate autonomously and uphold their public mission.

Panellists' contributions

Cecilia Rikap, University College London

Cecilia Rikap examined the concept of university autonomy, arguing that it encompasses multiple dimensions, including institutional, intellectual and financial autonomy. She highlighted the central role of financial dependence in shaping universities' choices and questioned dominant narratives that position innovation primarily within large technology and pharmaceutical companies. Rikap stressed the importance of distinguishing invention from innovation and argued that universities should play a more active role in shaping technological development according to public rather than commercial priorities.

Natali Helberger, University of Amsterdam

Natali Helberger framed digital sovereignty as a collective challenge that is reinforced through everyday technological choices. Drawing on experiences within the AlgoSoc consortium, she reflected on the difficulties of reducing dependence on dominant technology providers even when alternatives better align with academic values. She discussed the consortium's Nextcloud

pilot by SURF, emphasising the appeal of European, open-source infrastructures and noting the considerable institutional effort required to move from principle to implementation.

Wladimir Mufty, SURF

Wladimir Mufty approached the issue from a supply side perspective. He argued that digital sovereignty should not be understood as an all-or-nothing concept but as a spectrum of autonomy and control. While acknowledging the practical challenges of moving away from dominant providers, he emphasised the importance of maintaining innovative capacity and avoiding forms of vendor lock-in. Distinguishing autonomy from freedom of choice, Mufty suggested that universities must clearly identify the values they seek to protect and align technological choices with those priorities.

Michael Veale, University College London

Michael Veale focused on institutional governance and the relationship between technological choices and university autonomy. He argued that universities should evaluate technologies according to how well they serve academic needs rather than their novelty or market appeal. Veale also reflected on the difficulties universities face in coordinating collective action and developing shared infrastructures. He called for greater attention to infrastructural governance and the increasing concentration of control over both software and hardware environments.

Summary of Q&A discussion

The audience discussion focused on how far universities can realistically move away from dominant commercial infrastructures. Several interventions reflected on the difficulty of replacing deeply embedded systems used for research management, publishing workflows, and everyday administrative and teaching tasks. This led to questions about whether dependence on Big Tech tools is now mainly structural rather than a matter of institutional preference, and why alternatives are still so rarely taken up even when they exist.

In response, the discussion returned repeatedly to the need to understand dependency at the level of broader political and economic structures rather than individual tool choices. Speakers and participants highlighted issues such as fragmented decision-making within universities, weak coordination across institutions, and the reliance on a small number of committed actors to drive change. The role of public funding and state support was also raised, particularly in relation to whether universities can realistically be expected to transition to alternative infrastructures without long-term investment and political backing.

Panel Questions

How deeply does infrastructural dependency affect academic freedom?

The discussion highlighted that dependency on digital infrastructures affects academic freedom in ways that extend beyond privacy and security concerns. Speakers linked infrastructural dependence to broader questions of institutional autonomy, research priorities, and control over academic environments. Concerns were raised that reliance on dominant technology providers

may gradually shape the values, incentives, and forms of knowledge production within universities.

What are the obstacles to digital sovereignty for universities and research institutions and why it is so difficult to choose alternatives?

Several obstacles emerged throughout the discussion, including financial constraints, organisational inertia, lack of coordination between institutions, and existing forms of vendor lock-in. Panellists noted that alternatives often require significant investments of time, expertise and resources before they become viable. The challenge was described not only as technical but also cultural, as dependence on dominant providers can narrow institutions' sense of what alternatives are possible.

What could make a change? What tools do we have and are they actually helpful?

Open-source infrastructures, collaborative procurement, shared public-interest technologies, and greater cooperation between universities were repeatedly identified as potential avenues for change. The discussion stressed that alternatives already exist in many areas, but their adoption requires institutional commitment, technical support and long-term investment. Participants also emphasised the importance of developing narratives around public value rather than efficiency alone when evaluating technological choices.

Which is the one thing that policy makers and/or regulators must do?

The role of public institutions emerged as a recurring theme. Rather than focusing solely on regulation, speakers highlighted the importance of supporting institutional autonomy through sustained investment in public-interest digital infrastructures and alternative technological ecosystems. Funding, coordination and long-term strategic support were presented as necessary conditions for reducing dependence on dominant technology providers and strengthening universities' capacity to make independent technological choices.

Moderator: Maria Luisa Stasi, Article 19 - MLS

Panellist 1: Cecilia Rikap, University College London - CR

Panellist 2: Natali Helberger, University of Amsterdam - NH

Panellist 3: Wladimir Mufty, SURF - WM

Panellist 4: Michael Veale, University College London -MV

Rapporteur: Sruthi Vanguri, University of Amsterdam

CPDP 2026
19th international conference

19-22 May ■ Brussels, Belgium
COMPETING VISIONS, SHARED FUTURES

AI Sovereignty from the Global Majority

Date: 21 May 2026

Panel Organiser: FGV

Moderator's Introduction

Nicolò Zingales opened the session by situating the panel within an ongoing project at FGV on digital sovereignty and artificial intelligence, noting that their book on the subject, currently available in Portuguese with an English edition forthcoming, informed the framing of the discussion. In the book, they proposed a move away from the Westphalian conception of sovereignty as state control over territory and population towards a bottom-up understanding in which sovereignty belongs to the people and the state's role is to catalyse its citizens' capacity to develop and govern their own technologies. He emphasised that technological autonomy is not merely a policy aspiration but a constitutional duty under Brazilian law. The panel would explore this systemic understanding through a 'STACK approach', encompassing not only legal instruments but also code, societal norms, and economic incentives, on the basis that genuine independence cannot be achieved by focusing on any single technology layer in isolation.

Panellists' contributions

Cecilia Rikap, University College London

Zingales opened with the question of how digital dependence manifests in Latin America. Rikap argued that contemporary capitalism operates through a hegemonic system in which a small number of large technology corporations control the infrastructure and direction of knowledge production globally. She described the cloud market as a "supermarket of digital technologies" through which big tech companies exercise panoptical power and buy up the smaller companies to internalise their own services, extending their control across the economy. By 2024, she noted, thousands of start-up companies producing AI-relevant knowledge were financially dependent on the same large corporations whose cloud infrastructure they relied upon to operate, creating a deeply extractive and self-reinforcing hierarchy. This dependence extends to governments, which increasingly rely on proprietary AI systems provided by large technology firms, generating political dependencies that translate into local privileges and foreign protections for those corporations. She further observed that the United States conditions technology adoption by partner countries, framing it as diplomatic alignment while enabling data extraction and,

increasingly, the extraction of natural resources. Rikap argued that digital sovereignty is therefore both a territorial and a democratic question, requiring political imagination at international and local level. Her proposed starting point was decoupling the public sector dependence on these big tech platforms to conduct their services, beginning with sensitive domains such as education, where the stakes for children and society are highest.

Divij Joshi, ODI Global

Joshi offered the Indian perspective, defining digital sovereignty in the Indian context primarily as a projection of state power in the digital economy, whilst acknowledging that a more democratic conception, centred on individual sovereignty and participatory governance, would be normatively preferable. He explained that sovereignty discourse has intensified in India precisely because the state has come to recognise the extent of its dependencies, first on platforms and now on artificial intelligence, a shift thrown into sharp relief by geopolitical rivalries between the United States and China and, more recently, by national security anxieties following the emergence of models such as DeepSeek. The framing of sovereignty in Indian policy has evolved from an earlier emphasis on data localisation and the ownership of cloud infrastructure towards a more pronounced industrial policy focus aimed at fostering local AI companies and brokering cooperation and knowledge transfer between large international firms and domestic enterprises. Joshi was critical of this trajectory: the model prioritises industry promotion over governance, safety, and regulatory frameworks that would protect workers and consumers, and it entrenches a structurally unequal role for the Global South in the AI value chain. He characterised the arrangement as extractive and non-participatory, reproducing patterns already established in the platform economy. Joshi concluded by arguing that a genuinely progressive vision of digital sovereignty must go beyond asserting that the Global South has been left behind; it must articulate what a democratic alternative would look like and identify the structural drivers of extractive practices that need to be addressed.

Melody Musoni, European Centre for Development Policy Management

Musoni drew on her work across African countries and at the level of the African Union to trace how understandings of digital sovereignty on the continent have evolved over time. In the early stages of policy debate, she noted, digital sovereignty was largely equated with data localisation, a position shaped by a limited appreciation of what the data economy entails; policymakers were primarily concerned with preventing data from leaving the country rather than with extracting economic value from it. That understanding has gradually matured, enabling more nuanced conversations about how to leverage data and digital infrastructure for development. She introduced a framing that has resonated particularly well with African audiences: rather than describing data as “the new oil”, which conveys little intuitive meaning, she prefers the analogy of soil; something that must be protected, cultivated, and whose value should accrue locally before being exported. The central challenge now is identifying how economic value from data can be created and retained for local communities rather than flowing predominantly to international private-sector actors and large technology firms, a pattern confirmed by her field interviews.

Musoni discussed the significant gap in data centre infrastructure, Africa accounts for only approximately two per cent of global data centre capacity, and explored the case for regional

cloud solutions, or “data embassies”, as a means of reducing dependence on foreign actors whilst avoiding the inefficiencies of purely national approaches. She also highlighted a widespread misconception: African data is abundant but is largely held offshore by foreign governments and private entities, raising fundamental questions about who actually exercises sovereignty over it. She closed by arguing that the African priority is not winning any global AI race but positioning the continent to extract genuine economic and social value from developments in AI.

Sebastiano Toffaletti, Digital SME Alliance

Toffaletti brought the perspective of European small and medium-sized enterprises, endorsing the diagnosis offered by his fellow panellists and reflecting on two decades of European policy treating technology as a commodity rather than as a source of power. He agreed that cloud computing lies at the centre of the current technological order and cautioned against the assumption that building data centres in Europe is sufficient: what American hyperscalers have constructed is a vast ecosystem of services running on top of cloud infrastructure, and replicating the physical layer without the services layer does not enable switching or genuine competition. He identified the root problem not as technology per se but as the monopolistic structure of the current market, arguing that introducing democratic principles into market design would produce more democratic technologies. His proposed solution is a federated and interoperable European stack built by many SMEs, each contributing components, so that the stack grows organically and remains resilient, if any one firm fails, others can step in, unlike a single corporate provider. This federated model would also be modular and exportable: other regions, including African countries, could selectively adopt components suited to their needs and eventually develop their own alternatives. Toffaletti insisted that such an outcome requires strong alignment between the public and private sectors and active government leadership, since the highly fragmented European market, with thousands of companies none of which can individually compete with large technology firms, will not self-organise without political direction compelling interoperability and cooperation.

Summary of Q&A discussion

Question 1: Open Mind Foundation. Attendee raised the tension between open source advocacy and political reality, European governments still run largely on Windows, and Linux adoption in government has largely failed. The question posed: if open source keeps failing in Europe, why would it be different now?

Answers:

Cecilia Rikaap: Agreed this is fundamentally a political problem, not a resource one. Defense funding was offered as an example of how money materialises quickly when political will exists. The same logic applies here, if open source is genuinely prioritised through regulation, it becomes achievable. Where there is a will, there is a way.

Question 2: Access Now. Following a presentation on alternative cloud models, the question was: what is the regulatory vehicle that could realistically deliver this change? Does it fall under the DMA, a review process, or does it require an entirely new initiative?

Answers:

Cecilia Rikaap: The DMA is not the answer, it is difficult to implement, and the Commission is unlikely to act with the boldness required. The preferred solution is industrial policy: mandating that public procurement only purchases from EU-based cloud providers that comply with defined interoperability standards. This would naturally favour compliant companies and create market incentives for others to follow.

Moderator added that open source would also bring auditability, transparency, and security benefits, you cannot properly assess what you cannot inspect.

Sebastiano Toffaletti cautioned that while open source supports sovereignty, mandating open source exclusively would eliminate around 80% of the industry.

Cecilia Rikaap noted that open source is not automatically auditable either, LLMs were cited as an example where this falls short.

Question 3: Build Up. Attendee raised the question of whether AI is genuinely needed, particularly in the African context. However, they noted that people in rural African villages are already being exposed to LLMs, finding value in them, and actively requesting AI-powered tools for local sense-making. The question became: how do we keep space open for locally built LLMs to meet this demand?

Answers:

Cecilia Rikaap: People want AI, and big tech is already providing it. The answer is to push open source approaches through regulation and build the markets that flow from that.

Melody Musoni noted that Africa has data protection regulation for personal and non-personal data, but nothing specific to AI and even existing data regulation is difficult to enforce. AI regulation is not currently a priority on the continent.

Melody Musoni also highlighted that African LLMs do exist, referencing Deep Learning Indaba as a forum where innovators and SMEs connect with investors.

Divij Joshi raised a concern about dependency risk: much of current AI provision is built on artificially low pricing designed to create structural dependency, after which prices are increased significantly. This dynamic warrants close attention.

Panel Questions

What does AI sovereignty mean from the perspective of the Global Majority, and how does it differ from dominant perspectives?

The panel's starting point, set out by the moderator, was a deliberate move away from the Westphalian conception of sovereignty as a state's control over territory and population towards a bottom-up understanding in which sovereignty belongs to the people and the state's task is to cultivate its citizens' capacity to build and govern their own technologies, an autonomy he noted is treated as a constitutional duty under Brazilian law. Rikap sharpened the contrast with the dominant order, describing a hegemonic system in which a handful of large technology

corporations direct global knowledge production through what she called a ‘supermarket of digital technologies’, and arguing that sovereignty is therefore at once a territorial and a democratic question that demands political imagination rather than mere market participation. Joshi cautioned that the term is used in more than one way: in Indian policy it functions largely as a projection of state power in the digital economy, whereas the normatively preferable conception would centre individual sovereignty and participatory governance, and he insisted that a progressive account must go beyond complaining that the Global South has been left behind to articulate a democratic alternative and name the structural drivers of extraction. Musoni added the developmental register that, in her account, distinguishes the Global Majority view most clearly, preferring the image of data as soil to be protected and cultivated so that its value accrues locally over the familiar ‘new oil’ metaphor, and stressing that the African priority is not to win any global AI race but to capture genuine economic and social value at home. Running through these contributions was a shared conviction that sovereignty in this setting is people-centred and development oriented and so differs both from the state-control model and from the Western tendency, as Toffaletti put it, to treat technology as a commodity rather than as a source of power.

Which Key Sovereignty AI Enablers (KASE) are essential for building a sovereign AI Stack, and how are Global Majority countries addressing them in practice?

The moderator opened these questions by asking panellists to weigh the elements of a comprehensive sovereignty stack, which he defined as independent data governance. This includes the software, the algorithmic layers, the computational capacity, meaningful connectivity, electrical power, natural resources, digital literacy, cybersecurity and even regulation. The panellists responded by mentioning different enablers according to their regions. Rikap treated the auditability of computers as non-negotiable, arguing that any data centre a host country cannot inspect operates in effect as a ‘military base’, an instrument of foreign influence that generates no local employment, and she urged states to begin from what their populations actually need rather than from the assumption that everyone requires generative AI. Toffaletti warned that hardware alone is a trap, since what the American hyperscalers have built is a vast services ecosystem running on top of the cloud, so that replicating the physical layer without the services layer delivers neither switching nor competition. He suggested a federated, interoperable stack assembled by many SMEs under common standards and backed by procurement rules that buy only from EU compliant domestic providers, an arrangement he was clear would have to be mandated rather than left to emerge. Musoni grounded the question in African realities, noting that the continent holds only around two per cent of global data-centre capacity, that much African data is abundantly stored offshore by foreign governments and firms, and that regional cloud arrangements or ‘data embassies’ offer a way to reduce dependence without the inefficiency of purely national approaches. On regulation she observed that African states generally have data-protection rules, but nothing tailored to AI and that enforcement is difficult and could hinder development of an African Stack.

What lessons can be drawn from the experiences of countries such as Brazil and India in pursuing AI sovereignty amid structural asymmetries in data, compute, and infrastructure?

The Indian and Brazilian trajectories were presented as instructive in different ways. Joshi read the Indian experience largely as a cautionary one: sovereignty discourse intensified there as the state recognised the depth of its dependence, first on platforms and then on AI, sharpened by US–China rivalry and by security anxieties around models such as DeepSeek, and policy shifted from data localisation and cloud ownership towards an industrial policy of nurturing domestic AI firms and brokering knowledge transfer with large international companies. His criticism was that this model places industry promotion ahead of governance, safety and the regulation that would protect workers and consumers, and so risks reproducing the extractive, non-participatory patterns of the platform economy while entrenching the Global South's subordinate place in the value chain. The Brazilian framing, set out by the moderator and developed by Rikap, pointed the other way, casting technological autonomy as a constitutional duty and sovereignty as a bottom-up, democratic project, with Rikap proposing that the public sector begin to decouple from the dominant platforms in the most sensitive domains first, education among them. The common lesson the panel drew was that asserting sovereignty is not sufficient in itself unless the structural drivers of dependence are confronted. Joshi's insistence that the real task is to articulate a genuinely democratic alternative, rather than simply to protest being left behind, captured the point on which the Brazilian and Indian lessons converged.

To what extent can cooperation among Global Majority countries foster a multipolar and development-oriented model of AI governance?

On the prospects for cooperation the panel was cautiously constructive, seeing real potential alongside firm limits. Musoni made the case that some degree of international partnership is unavoidable while developing the necessary infrastructure. She described the delicate diplomacy this entails, from managing the legacy of Huawei infrastructure to balancing US and Chinese influence all the while having the EU serve as a regulatory reference point. Although, she notes that too often these countries advance their initiatives for what AI should be in Africa without consulting African partners, breeding scepticism about externally driven investment packages. Toffaletti argued that his federated stack idea is deliberately modular and exportable, so that other regions, African countries included, could selectively adopt the components that suit them and in time build their own, which points to a practical basis for South–South and cross-regional cooperation rather than dependence on any single provider. Rikap located the same ambition at the level of political imagination, treating sovereignty as a democratic question to be pursued internationally as well as locally, while Musoni framed the shared goal as genuine value creation through authentic knowledge and technology transfer over time rather than victory in an AI race. Joshi closed with a provocation by suggesting that cooperation might be better directed at imagining a different AI ecosystem altogether. He explained that the current AI system is highly centralised, like with nuclear power, and argues that we should rethink to make a more flat and democratic AI system, much like solar energy, where local actors can create hardware, software, and run AI in a cooperative manner. The panel's tentative answer was thus that cooperation can indeed support a more multipolar and development-oriented model, but that the shape it takes needs to differ, taking a more locally grounded alternative rather than the current centralised AI order.

Moderator: Nicolo Zingales, Professor at FGV - NZ

Panellist 1: Cecilia Rikaap, University College of London - CR

Panellist 2: Divij Joshi, ODI Global, DJ

Panellist 3: Melody Musoni, European Centre for Development Policy Management - MM

Panellist 4: Sebastiano Toffaletti, Digital SME Alliance - ST

Rapporteur: Matteo Bard, University of Amsterdam