CPDP 2026

Session Reports

Day 3

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

The U.S. Deregulatory Effect on Global Lawmaking, Policy, and Enforcement

Date: 22 May 2026

Panel Organiser: EPIC

Moderator's Introduction

Maria Villegas Bravo introduces this panel, which examines the evolving landscape of technology deregulation in the U.S. and internationally, with particular attention to the influence of major technology companies on policymaking. The panel considers the role of litigation in the U.S., where existing technology-related legislation and state-level regulatory initiatives are frequently challenged by large technology firms. The discussion addresses the growing influence of corporate lobbying and political advocacy on technology policy, as well as their implications for future regulatory frameworks and democratic governance. Finally, it also explores shifting dynamics in transatlantic relations, including changes in regulatory cooperation between the U.S. and the EU amid broader geopolitical and economic developments.

Panellists' contributions

Alexandra Geese, European Parliament

Alexandra Geese contends that industry actors exert substantial influence over policymaking processes. These actors are shaping regulatory agendas through narratives of simplification and participation in policy dialogues, thereby raising concerns about regulatory capture and the protection of fundamental rights in the digital sphere. She states that the primary challenge in digital governance, however, is insufficient enforcement of existing measures, rather than the absence of regulatory frameworks. For example, in terms of platform regulation, while regulatory efforts on transparency and online speech are important, the slow pace and perceived ineffectiveness of investigations into related harms have undermined public confidence in regulatory institutions. These delays in enforcement also weaken democratic legitimacy. Moreover, Alexandra Geese challenges the argument that regulation is responsible for economic or technological underperformance, arguing instead that inadequate regulation and oversight can generate significant social harms and erode public trust. Thus, she advocates reframing the policy debate, emphasising that effective regulation serves a protective function by mitigating

risks, safeguarding public interests, and creating conditions for more sustainable and responsible innovation.

Tomaso Falchetta, Privacy International

Tomaso Falchetta's discussion extends beyond the EU and the U.S. to examine the broader global implications of digital regulation and deregulation. He notes that while the U.S. has pursued an increasingly assertive agenda to reshape international digital governance frameworks, the EU appears to be shifting toward a discourse of regulatory simplification that may weaken certain existing safeguards. At the same time, comparative evidence suggests that regulatory developments are shaped not only by external pressures but also by domestic political and economic dynamics, resulting in varied outcomes across jurisdictions. Examples from countries such as India and Brazil illustrate how both multinational technology firms and local industry actors influence policy debates, while governments continue to negotiate competing demands for market regulation, competition, and innovation. Overall, the evolving landscape of digital governance reflects a complex interplay among international influence, domestic interests, and institutional capacity, producing divergent trajectories of technology regulation across regions.

Michael Veale, UCL Faculty of Laws

Michael Veale discusses the issues through the lens of the UK. He argues that U.S. international influence on digital governance operates through both direct political pressure and broader normative effects. Such influence shapes legislative agendas, regulatory interpretations, and policy debates. For example, the development of the UK's AI governance framework, including the establishment of the AI Security Institute, has been influenced by U.S.-based political networks. More broadly, he contends that deregulation increasingly operates through informal channels of influence and micro-level intervention, such as pressure from both technology firms, shaping policy outcomes and constraining regulatory ambitions in the UK.

Calli Schroeder, EPIC

Calli Schroeder notes that the deregulation agenda in the U.S. has become pervasive, affecting federal agencies and legislative processes, with some institutions being weakened, rendered ineffective, or directed to curtail regulatory activities. In response to perceived federal inaction, state governments have pursued regulatory initiatives. However, these efforts are increasingly shaped by technology companies, which influence policymaking through coordinated lobbying and the dissemination of industry-generated policy arguments. Calli Schroeder further contends that deregulatory efforts extend beyond domestic governance, encompassing the use of trade and contractual agreements to encourage other countries to adopt more permissive regulatory frameworks favourable to U.S. technology firms. She also compared the international approaches to AI governance, arguing that structural differences between the U.S. and the EU (such as social welfare systems and exposure to AI-related risks) shape public sentiment and regulatory responses. Overall, Calli Schroeder concludes that industry priorities in the U.S., particularly the emphasis on rapid innovation and revenue generation, have constrained the adoption of robust, safety-oriented AI governance frameworks despite growing awareness of the associated risks.

Summary of Q&A discussion

Question 1: A lawyer from China

1. To what extent do intra-national political tensions in the U.S. have the potential to influence federal regulatory approaches, especially in relation to AI governance, in the context of upcoming midterm elections?
2. How is the evolving 'special relationship' between the UK and the U.S. affecting the UK's strategic alignment in digital regulation, and to what extent is the UK moving closer to either the EU or the US regulatory model?
3. In what ways might geopolitical competition with China, alongside prevailing anti-China sentiment, shape the U.S.'s regulatory stance on technology, and could this dynamic contribute to a shift toward a more pro-regulatory approach in AI governance?

Answers:

Calli Schroeder: While structural divisions between U.S. coastal tech and regulatory ecosystems are notable, anticipated political shifts are more likely driven by broader dissatisfaction with perceived corruption and governance under the Trump administration. Additionally, the U.S. AI policy discourse, particularly in relation to China, is increasingly shaped by nationalist and racialised framings. However, such strategies appear to have limited effectiveness in securing public support for deregulation, given widespread public demand for stronger AI protections and regulation.

Michael Veale: As for the second question, the UK courts have demonstrated an ongoing effort to engage with and informally align their reasoning with post-Brexit Court of the CJEU judgments. As for the Chinese issues, certain Chinese regulatory approaches to AI demonstrate comparatively advanced and systematic responses to emerging technological risks, despite significant concerns about censorship and fundamental rights. The dominant geopolitical narratives framing the U.S. as deregulatory, Europe as regulatory, and China as uniformly repressive are overly simplistic. After all, jurisdictions exhibit varied and evolving regulatory innovations that warrant deeper comparative analysis.

Question 2: Is the functioning of civil society affected by this trend?

Answers:

Calli Schroeder: In the US, civil society engagement in government policymaking has significantly diminished, evidenced by the exclusion of civil society actors from formal consultation processes. They are being replaced by industry-aligned groups, and substantial reductions in federal funding have undermined the operational capacity and sustainability of many civil society organisations.

Alexandra Geese: While challenges to civil society are primarily domestically generated, they are worsened by strategic and operational methods originating from U.S. political contexts, particularly those associated with far-right organising and procedural tactics within institutional settings.

Tomaso Falchetta: These developments are not solely attributable to U.S. influence but are also shaped by domestic legislative initiatives.

Question 3: How do we maintain the EU's resilience?

Answers:

Alexandra Geese: Sustaining democracy requires a persuasive articulation of its benefits to the public, and it is necessary for political actors to effectively communicate and justify democratic governance.

Panel Questions

How can the U.S. be deregulating when they do not have a federal privacy law to begin with?

Even in the absence of a federal privacy law, the trend of deregulation can still affect federal agencies, enforcement bodies, and legislative processes. Specifically, it can weaken institutional capacity, reduce regulatory effectiveness, or redirect public authorities toward limiting regulatory intervention. Beyond the federal level, deregulation also affects state-level policymaking, as technology companies shape regulatory outcomes through coordinated lobbying and the dissemination of industry-generated policy narratives and proposals.

Is EU simplification a reflection of the U.S. deregulatory approach?

Not necessarily. Even though the U.S. deregulatory approach does affect the EU approach, there are inherent structural factors that shape the EU simplification. For example, social welfare systems and exposure to AI-related risks contribute to the current EU public sentiment and regulatory responses.

How do trade agreements, tariffs, and other factors play in to deregulatory decision making?

The influence of the U.S. on international digital governance operates through both direct political pressure and broader normative mechanisms, shaping legislative agendas, regulatory interpretations, and policy debates across jurisdictions. Increasingly, deregulatory influence is exercised through informal channels, including agenda-setting, policy diffusion, and micro-level interventions within regulatory and legislative processes. At the same time, regulatory developments are determined not only by external pressures from the U.S. but also by domestic political, economic, and institutional dynamics. Consequently, the evolving landscape of digital governance reflects a complex interaction among international influence, domestic interests, and state capacity, resulting in diverse and uneven trajectories of technology regulation across regions.

Are there countries that are holding firm or responding with MORE regulation and enforcement to this U.S. approach?

The Chinese approach to AI regulation is considered a comparatively firmer and systematic response to emerging technological risks, notwithstanding significant concerns regarding censorship, state surveillance, and the protection of fundamental rights. Nevertheless, prevailing geopolitical narratives that characterise the U.S. as primarily deregulatory, Europe as

predominantly regulatory, and China as uniformly repressive are overly reductive. In practice, each jurisdiction exhibits diverse and evolving forms of regulatory innovation, highlighting the need for more nuanced comparative analysis and greater cross-jurisdictional learning.

Moderator: Maria Villegas Bravo, EPIC - MVB

Panellist 1: Calli Schroeder, EPIC - CS

Panellist 2: Tomaso Falchetta, Privacy International - TF

Panellist 3: Alexandra Geese, European Parliament - AG

Panellist 4: Michael Veale, UCL Faculty of Laws - MV

Rapporteur: Ting-Yu Yu, the University of Edinburgh

CPDP 2026
19th international conference

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

Digital Omnibus meets the Charter of Fundamental Rights – a reality check

Date: 22 May 2026

Panel Organiser: noyb

Moderator's Introduction

Jennifer Baker, journalist and presenter, opened the panel with a very brief introduction bringing up a reality check on the Digital Omnibus proposal as Parliament begins deliberations and the Council's second compromise text already removes several key provisions, prompting widespread concern from stakeholders. Many argue that the proposal creates legal uncertainty, increases workload, and even limits users' rights rather than simplifying the framework. The moderator also flags a risk of mission creep, questioning whether the Omnibus remains within Charter-compliant boundaries or exceeds the legislature's mandate.

Panellists' contributions

Herwig Hofmann (University of Luxembourg) began the panel in which he outlined four core issues. First, he highlighted the definition of the scope and possible limitations of Article 8 CFR protection within the Digital Omnibus Act, noting how unusual it is for secondary legislation to attempt to delineate the boundaries of a fundamental right. Second, he stressed that any such limitations must meet the proportionality requirement and that this assessment depends on robust impact assessments, an element that is conspicuously absent. Third, he pointed to fundamental legal principles such as legal certainty and non-retroactivity, especially regarding data already collected and used to train AI models. Fourth, he questioned the extent to which powers can be delegated to the Commission: determining the scope of fundamental rights protection is an essential element that cannot simply be handed over through delegated acts. He closed by noting that the proposal also introduces significant limitations to GDPR rights of access, raising a broader set of rights-related concerns.

Alexandra Jaspar's (Data Protection Authority of Belgium, Director of the Authorization and Opinion Service, member of the Executive Committee) presentation focused on Articles 12(5), 13(4), and 15, grounding her analysis in Article 8 of the Charter, which explicitly guarantees everyone an unconditional right of access to their personal data. She noted that the proposed Article 12(5) would restrict access requests to situations in which individuals seek to "check"

their data or verify compliance, which, to her, is an unjustified narrowing of a fundamental right. Under Article 52 CFR, any limitation must be necessary, proportionate, and genuinely meet an objective of general interest. Jaspar questioned whether such a necessity exists: are organizations truly overwhelmed by access requests, and even if so, would that justify curtailing a Charter right? She illustrated this with the example of a worker seeking to verify data used in a lay-off decision, precisely the kind of situation where broad access is essential. She stressed that proportionality is entirely unsubstantiated in the proposal: how would a controller assess the intent of the requester, and must a data subject now motivate their access request? Nothing in the GDPR requires such justification.

Turning to Article 13(4), she warned that the proposal lowers the controller's burden of proof for refusing requests, even though the GDPR already allows refusals for manifestly unfounded or excessive requests. Article 12(5), in its current form, introduces vague notions such as overly broad and undifferentiated requests, which risk shifting responsibility onto the data subject. She concluded by asking why individuals should have to be specific when the very purpose of an access request is to understand what data the controller holds about them

Max Schrems (noyb) questioned the legitimacy of the Council's approach, noting parallels with an ongoing debate in Germany about whether individuals should be prevented from generating information they would not otherwise have, despite this being a core element of informational self-determination. He emphasised that Article 8 is not merely a data-protection rule but an enabler of other fundamental rights, which makes restrictions particularly sensitive.

The Moderator then asked Max as to how legitimate is the Council's idea of treating not only data-subject access requests but also complaints to supervisory authorities as potentially abusive or made with abusive intent? Max warned that the proposal seems designed with the assumption that complaint authorities act abusively, even though EU law already contains a general principle prohibiting abuse of rights. Schrems asked why this principle needs to be restated or expanded here, suggesting that the proposal risks over-correcting a problem that has not been demonstrated.

Jennifer then asked Rosalia Anna D'Agostino (Spirit Legal) is this proposed limitation on access rights actually necessary, and what is the practical justification for it in real-world terms? Rosalia stressed that, especially in the age of AI, access to one's data is essential for understanding how that data is used and for exercising meaningful control over it. Building on Max's point about informational self-determination, she underlined that individuals have the right to decide what others know and do not know about them. The right of access is therefore not a procedural nicety but a core component of the broader right to self-determination.

Jennifer asked Herwig Hoffman whether there are, in practice, cases of annoying or burdensome access requests. He acknowledged that such cases exist but stressed that the mere exercise of a right does not constitute abuse. Access to one's data is intrinsic to the very purpose of the right: without access, individuals cannot make claims, challenge decisions, or exercise meaningful self-determination. He warned that attacking access rights and the ability to understand or contest data processing strikes at the core of Article 8 of the Charter. If individuals are subject to data processing but denied effective access, the fundamental right itself becomes hollow.

Jennifer asked Alexandra whether introducing a subjective element into access rights would make those rights harder to enforce. Alessandra replied that it inevitably would: the data subject would be forced to justify their intentions, and controllers would gain new grounds to refuse requests, despite already struggling to respond properly under the current GDPR framework.

Max then discussed two more elements of the Omnibus proposal. One element is the proposed exemption for SMEs from the privacy notice obligation fails the precision requirement under Article 52 of the Charter. Vague factors such as the depth of the processing do not provide the legal certainty necessary for a limitation on a fundamental right. Moreover, the exemption would apply to 99% of European businesses, thereby removing transparency, which is a core component of fair processing under Article 8 of the Charter, for the vast majority of data subjects. The other element was on the repurposing of research data. In this, the proposed definition of scientific research risks collapsing Article 13 Charter academic freedom into a broad innovation mandate, sidelining non-innovative disciplines while opening the door for commercial actors to invoke the research exemption for activities such as product optimisation. Because this redefinition is paired with the removal of Article 13 GDPR notice, it effectively disables the Article 21 opt-out and undermines the Article 51B purpose-limitation bargain, allowing sensitive data to be repurposed for secondary research without individuals ever being informed or able to exercise control an outcome that is difficult to reconcile with Articles 7, 8, and 52 of the Charter.

Finally, the last matter raised in the panel was on the matter of personal data and pseudonymization and anonymised data The core problem with the Omnibus proposal is that it attempts to generalize a highly fact-specific CJEU ruling on pseudonymization into a new, subjective definition of personal data, one that turns on a controller's own capacity and intentions. This creates what speakers described as a "data / non-data switching" problem: the same dataset could oscillate between being personal data and non-personal data depending on temporary technical configurations, software updates, or a controller's stated intentions. Such subjectification undermines legal certainty for both individuals and controllers. Individuals cannot know when their rights apply, and companies—especially SMEs—cannot reliably determine whether they fall within the GDPR or face liability under Article 82. It also collapses the GDPR's carefully calibrated distinction between pseudonymisation (Article 4(5), still personal data) and true anonymization (irreversible, outside scope). By allowing controllers to claim "subjective anonymisation" based on their own capabilities, the proposal effectively rewrites the regulation and erodes accountability.

Beyond legal certainty, the proposal raises deeper structural and constitutional concerns. Capacity and intent are fluid and easily manipulated, creating regulatory arbitrage: a controller could simply claim no intention to re-identify, or avoid developing certain capabilities, to escape the GDPR, even though the same dataset would clearly be personal data in the hands of another actor. This conflicts with the Charter's Article 8 understanding of personal data, which the CJEU has consistently interpreted through an objective test of identifiability by "means reasonably likely to be used." The legislature cannot redefine that core concept without entering into tension with the Charter. The practical consequences are stark: large parts of the ad-tech ecosystem, built on pseudonymous identifiers and cross-site singling-out, could fall outside the GDPR entirely by asserting a lack of re-identification intent. Meanwhile, the burden on SMEs becomes paradoxically heavier, as non-lawyer DPOs would be forced to navigate an unstable, subjective

threshold. In short, the proposal destabilises the foundational scope rule of EU data protection law, creating uncertainty, loopholes, and constitutional risk.

Summary of Q&A discussion

Question 1: (Farid Masouli, research at Raboud University) How does the omnibus proposal (especially the risks around anonymisation and secondary use) relate to the European Health Data Space (EHDS) regulation, which mandates anonymisation by default for secondary use, including AI training? The questioner is writing on legal basis problems in the EHDS.

Answers:

Max: At NOYB, we have not looked deeply into the health data space, so the answer will be limited. However, a key difference is that the omnibus proposal imposes no further limitations on secondary use: no mandatory anonymisation, no additional safeguards. The EHDS framework is more restrictive. There may be overlapping problems, but the legal architectures differ significantly.

Question 2: (Danny Hooksma, a data protection lawyer) Regarding the proposed limitation on Article 12(5) (right to a privacy notice) – how do you interpret that in light of the recent Britt Rottler case and the growing practice of constructing situations to claim damages? Is this a problem we should solve or just collateral damage of the GDPR?

Answers:

Herwig: The first question is not new; the Court has already addressed many of the problematic aspects in its case law. The second question concerns Article 12(5), which the courts have also examined, and about which I remain doubtful—particularly given how closely it ties into our broader discussion on pseudonymisation and anonymisation from a technological perspective. Article 12(5) of the Omnibus proposal is drafted in sweeping and highly subjective terms. It also indirectly undermines Article 82 on the right to compensation. The deeper structural issue, however, is the increasingly blurred boundary between pseudonymisation and anonymization.

Question 3: What are your thoughts on data twins and how they are operationalised? The Data Governance Act provides a clear framework, but in practice, there are twins pushing vulnerable people to donate data on the basis of consent. What are your thoughts, and how will the omnibus effect this?

Answers:

Rosalia: Data twins can be useful for research and democracy. Some research has been done on how data twins could be used to enhance democracy. It is an interesting area of knowledge. The problem is that once a data twin is created, it is very difficult to separate the twin's data from the original person's data. Retrieving or deleting the data later is practically impossible. It is difficult to go back once they are created.

Question 4: (DPO from a German energy company) As a DPO, I receive massive numbers of needless Article 15 access requests, often generated by ChatGPT to annoy companies. The requests are very broad, making it hard to know where to search. I solve this by entering into a

back-and-forth dialogue to narrow the request. Could this approach be codified into Article 12 as a middle ground between a general request and a complete block?

Answers:

Alexandra: Codification is not necessary. This approach is already regarded as acceptable by any DPA. Recommended steps: (1) Use a filtering system, such as a web form that lets data subjects select what they are interested in. (2) Standardise your responses as most requests ask the same things. Your RoPA (record of processing) should already contain all the answers. (3) If a requester does not come back after a genuine dialogue, you may consider the request abusive.

Max: AI-generated requests are not just an Article 15 problem – DPAs are also flooded. The real issue is that some companies use prolonged debates (five months) to avoid answering genuinely. When done in good faith, limiting and narrowing works well.

Question 5: (Yuna – private lawyer, Netherlands) In the Netherlands, there are many alternative legal routes to access personal data (Freedom of Information Act, healthcare law, civil procedure code). Isn't the debate about Article 15 access rights somewhat academic or theoretical? Or is it truly operational?

Answers:

Max: It is extremely member-state dependent. In German-speaking countries (Austria, Germany), there is very limited pre-trial discovery. Lawyers therefore use Article 15 as a discovery tool. That is seen as abusive in national civil law traditions. This is a clash between European law and national legal traditions and European law prevails. There is a difference between an annoying request (e.g., from activists) and an abusive request (designed solely to extract damages). If your data is properly structured, handling these requests is manageable; the real burden falls on large-scale industries like telecoms and energy companies.

Alexandra: Belgium also has sector-specific access rights (e.g., to hospitals). The unique value of Article 15 is that it applies to any organisation without needing to go through a judge or discovery procedure saving time and money. The Commission's proposal includes a "reset" provision that would deem a request abusive if it is made with the intention of subsequently demanding compensation or settlement.

Panel Questions

Do proposed amendments to the GDPR in the Digital Omnibus conflict with the European Charter of Fundamental Rights and if so, why?

Yes, several proposed amendments in the Digital Omnibus conflict with the EU Charter of Fundamental Rights. The proposed Article 12(5) restricts the right of access under Article 8(2) CFR to situations where individuals need to justify their data access request, introducing subjective intent requirements that undermine the unconditional nature of the right and fail the necessity and proportionality test under Article 52(1) CFR. Vague criteria, such as the depth of the processing for SME privacy notice exemptions, lack the legal precision required for any limitation on a Charter right. Moreover, removing Article 13 transparency obligations while

expanding the definition of scientific research to include innovation severs the link between notice and the Article 21 opt-out, enabling secondary use of sensitive data without individuals ever being informed, a disproportionate outcome that is difficult to reconcile with Articles 7, 8, and 52 of the Charter.

What would be the impact of these changes regarding legal certainty and any potential subsequent annulment action?

The proposed changes would severely undermine legal certainty by introducing vague, subjective criteria that controllers and data subjects cannot reliably apply dilutes legal certainty. This imprecision directly violates the requirement under Article 52(1) CFR that any limitation on a fundamental right must be "provided for by law" with sufficient clarity and predictability.

Does the Digital Omnibus meet the Charters' conditions and limitations for amending fundamental rights?

No. Under Article 52(1) of the Charter, any limitation on fundamental rights must be provided for by law, respect the essence of the right, be subject to the principle of proportionality, and be necessary to meet genuine objectives of general interest. The

Should or can Omnibus-type law be used as regulatory tool to substantially amend EU legislation protecting fundamental rights?

The panel was unanimous that while an Omnibus law is procedurally possible, it is normatively inappropriate for amending fundamental rights legislation. The panellists argued that the Charter imposes a heightened standard of justification that cannot be met by the broad-brush, non-sector-specific approach of an Omnibus instrument. Moreover, the lack of detailed impact assessments per provision and the compressed legislative timeline prevent meaningful scrutiny by the European Parliament and civil society. The panel concluded that an Omnibus law should be used only for technical, non-substantive adjustments – not for weakening core Charter rights.

Moderator: Jennifer Baker, journalist and presenter - JB

Panellist 1: Herwig Hofmann, University of Luxembourg - HH

Panellist 2: Alexandra Jaspar, Data Protection Authority of Belgium, Director of the Authorization and Opinion Service, member of the Executive Committee - AJ

Panellist 3: Max Schrems, noyb - MS

Panellist 4: Rosalia Anna D'Agostino, Spirit Legal - RAD

Rapporteur: Pia Groenewolt, VUB LSTS

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

OSINT as artistic and legal tool for restistance

Date: 22 May 2026

Panel Organiser: Privacy Salon

Culture Club Discussion

Moderator's Introduction

Opening the panel, Alexandre Alaphilippe, director of the Brussels-based NGO EU DisinfoLab, situated OSINT within the wider struggle against disinformation and information manipulation. He noted that open-source investigation has gained striking visibility over the past decade, moving from an obscure acronym to a central tool in journalism, accountability work and counter-disinformation practice. Rather than define OSINT narrowly, Alaphilippe framed it through the question of what open data can make visible and how that visibility can be used. He emphasised the field's strongly visual character, from network maps to relationship diagrams that make complex connections legible. For Alaphilippe, this visual dimension pointed to the panel's central concern: how artistic and legal approaches to evidence, often treated as opposites, can intersect in documenting harm and producing accountability.

Panellists' contributions

Mark Cinkevich (remote speaker)

Mark Cinkevich, an artist, film director and anthropologist participating remotely, presented OSINT as a method informing his practice. He screened an excerpt from *Onset* (2023), a short film made with the artist Anna Engelhardt that brings together medieval demonology, open-source intelligence and CGI animation to reconstruct three Russian-operated air bases: Khmeimim in Syria, Baranovichi in Belarus and Belbek in Ukraine. Built from satellite imagery and online visual material, the film imagines these military sites as ominous synthetic environments through which a demonic, parasitic force moves, passing through deserted corridors, interrogation rooms and electricity substations. Rather than treating the bases simply as architectural structures, *Onset* figures them as organisms under possession: spaces penetrated by an external force that damages them from within. In this register of "infrastructural horror," Engelhardt and Cinkevich use fiction not to depart from research, but to make visible the violence of Russian colonialism and the hidden dependencies sustaining military occupation. Beneath

the speculative layer sits a factual core built through tracing dual-use power lines and consulting military experts, showing how these bases secure uninterrupted electricity at the expense of surrounding civilian infrastructure.

Cinkevich argued that this fictional layer counters the desensitisation produced by distant, “from-above” satellite perspectives, seeking instead to implicate the viewer and recover affect. He described research on a Russian-financed nuclear power plant in Belarus that revealed the country’s energy infrastructure to be wholly dependent on Russia, work he felt unable to publish under his own name. Artistic practice, he suggested, grants the freedom to take a stance and to explore a dynamic without producing a court-grade reconstruction. He closed with a recent OSINT built diagram that maps how the Belarusian state processes a digital file: a face captured by CCTV passes through a Ministry of Internal Affairs monitoring system into a central database whose software core comprises three Russian companies, with the National Centre for Traffic Exchange as the single chokepoint through which the state can sever the country’s internet. He noted that four cables now link Belarus to Russia after the connections to Ukraine were cut, that this synchronisation was retrospectively legalised by a 2023 cybersecurity decree, and that Belarus serves as a “laboratory state” for a cyber perimeter now extending across the Collective Security Treaty Organisation.

The panel then turned to a second screening: an excerpt from Forensic Architecture’s documentary *Digital Violence: Pegasus Stories*, focused on Pegasus spyware, the murder of Jamal Khashoggi and the targeting of his associates. Alaphilippe introduced the excerpt as an example of how investigative practice can both humanise a story and find visual forms for “dry” evidentiary data: dates, contacts, communications and connections between actors. He noted the film’s movement from two-dimensional mapping into three-dimensional visualisation, describing this as a way of rendering patterns of surveillance almost like the spread of infection. For him, the excerpt showed where investigation and art can meet: in the task of making technical data intelligible, spatial and affectively compelling. This led into Winny’s reflections through asking what was the perception of using OSINT at first as data for accountability.

Rachel Winny, , CIR Center for information resilience

Rachel Winny of the Centre for Information Resilience, a UK-based non-profit that conducts open-source digital investigations into rights violations, traced the evolution of OSINT from early optimism about the democratisation of information to the present condition of overload and commercialisation across newsrooms, militaries, private intelligence firms and governments. This shift, she argued, has made questions of method and ethics more urgent: the fact that information is publicly accessible does not mean it can be used without consequence. A photograph posted online, for instance, does not amount to consent for that image to be geolocated and linked to a person’s address. Winny also stressed that neither data nor investigative methods are neutral. Satellite imagery is plentiful for Ukraine but delayed or unavailable for places such as the Sahel and Iran, while social media privileges those who are online and can leave forms of violence, particularly violence against women indoors, unseen. Drawing on war-crimes documentation in Ukraine and a timeline reconstruction of violence against protesters in Myanmar, she described the tension between the dry, legalistic language required by courts and the human storytelling needed to make publics care. Investigators, she suggested, must decide what kind of accountability they are seeking and choose their form of presentation accordingly. Greater diversity among practitioners, together with screened open datasets that others can reuse, may help address these limits.

Tatsiana Ashurkevich, Independent Journalist

Tatsiana Ashurkevich, a Belarusian investigator based in London who works on Belarus and Russia alongside Christo Grozev, spoke from the perspective of investigative practice under direct threat. Subject to two wanted lists and six criminal cases across Belarus and Russia, she described exile as the condition that makes her work possible. From outside Belarus, she can use methods that would be impossible at home, including calling officials under an assumed identity; inside the country, the act of documentation itself can mark a person as an enemy. She reflected on working with "investigation enthusiasts" and partisan hackers who provide valuable material but often want to publish everything, requiring her to insist on safeguards for those who could be harmed. For Ashurkevich, OSINT sits between activism and journalism: it can draw on leaked or purchased data when investigating figures such as Lukashenko, Putin or state propagandists, but it must draw a firm ethical line around ordinary citizens.

Across the three contributions, a shared concern emerged: the choice between evidentiary and affective registers is not merely stylistic, but shapes what kind of accountability becomes possible. It is also conditioned by context: where an investigator works, what legal framework they address and what risks they personally face. A brief exchange over whether blood should be described as "red liquid" crystallised this gap. Ashurkevich found the formulation astonishing, while Winny acknowledged it as a product of the effort to make evidence court-proof. The panel ultimately converged on the need for careful collaboration over institutional ego, treating open-source investigation as a practice that depends not only on access to information, but on judgement, responsibility and trust.

Summary of Q&A discussion

Question 1: How much do you collaborate with these organisations (like Bellingcat), to what extent do you share your insights and data with them?

Answers:

The panellists were broadly positive but frank about the barriers. Winny said that the Centre for Information Resilience works closely with local organisations and diaspora communities, both to reduce risk and to bring in ground knowledge beyond a field historically dominated by Europe and the United States. Ashurkevich, speaking as a freelancer, noted that larger outlets often resist collaboration in pursuit of exclusivity, which is one reason she avoids tying herself to a single institution and instead works with trusted collaborators. Alaphilippe was more critical, pointing to the "badly placed ego" that prevents sharing and citing coverage of the Russian "Doppelganger" operation, where many new publications simply repeated existing findings, and where ultimately you need to think about what's your added value. For him, collaboration sustains the open-source community, even when it takes the limited form of sharing tips rather than formal partnership.

Question 2: On data privacy and protection – publishing personal data of "the bad guys".

Answers:

A second question asked whether the reluctance to publish personal data about "the bad guys" reflected only the specific pressures of the Belarusian context, or also a broader difference in attitudes toward data privacy. Cinkevich traced the issue back to 2020, when the Belarusian state

created databases and Telegram channels to de-anonymise protesters, and the opposition responded in kind through initiatives such as the "Black Book of Belarus," exposing police officers. He described these competing archives as rival "bestiaries": lists through which each side cast the other as monstrous and fought over who counted as normal. In that context, he suggested, data exposure became part of a wartime logic in which "all weapons are good," even if the ethics remain troubling. Ashurkevich echoed this asymmetry from the perspective of an investigator working on Russian and Belarusian state power. She said she gives little weight to the privacy of Lukashenko, Putin, propagandists and others who support violence in Ukraine and Belarus, but maintains a distinction between those in power and ordinary citizens. Cinkevich added that many practitioners are personally implicated in the systems they investigate; in Belarus, documentation can be a matter of survival, which produces a different level of motivation. Winny, by contrast, emphasised the geography and legal framework of publication. As a UK-based investigator, she must demonstrate GDPR compliance, conduct data-protection impact assessments and navigate other risks, which can require stripping out material even when it could be defended in court.

Question 3: Can data markets and botnets usefully complement OSINT in investigative journalism and artistic research, or should OSINT remain "pure" and avoid these methods?

Answers:

The final question, prompted by an earlier session on data markets and botnets, asked whether these methods can complement OSINT or whether open-source research should remain "pure." Winny described this as a constant weighing of justification against complicity. Publicly available leaked data may be usable, but buying data from criminal marketplaces or the dark web sets a much higher ethical threshold, since it risks supporting the system that produced the data. She raised similar concerns around ad-tech data: although it can be powerful for exposing repression, it is also intrusive surveillance data, so organisations need clear principles for deciding when the ends justify the means. Ashurkevich took a more direct position, arguing that these methods do complement OSINT and that, in the Russian context, buying data is a common investigative practice. She said she would not buy information on ordinary citizens, but would do so on propagandists, Putin or Lukashenko, because those actors operate without "red lines" and should not be able to rely on journalists' restraint. Alaphilippe added that such material can play a limited investigative role: even when it is not published, it may serve as a signal that confirms a hypothesis or guides further open-source research.

Moderator: Alexandre Alaphilippe, EU DisinfoLab - AA

Panellist 1: Mark Cinkevich (remote speaker) - MC

Panellist 2: Rachel Winny, CIR Center for information resilience - RW

Panellist 3: Tatsiana Ashurkevich, Independent Journalist - TA

Rapporteur: Megan Leal Causton, Vrije Universiteit Brussel

CPDP 2026
19th international conference

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

Data-driven warfare: AI, civilian risks, and corporate responsibility

Date: 22 May 2026

Panel Organiser: Privacy International

Moderator's Introduction

The moderator opened the session by welcoming attendees to the panel, co-organised with Article 19, which examines how civilian data-driven tools are being repurposed for military use and how military technologies are quietly reshaping civilian infrastructure. Artificial intelligence sits at the centre of this blurring boundary, with targeting systems now operating at a speed and scale that effectively strips away meaningful human oversight. The same technologies are then redeployed in civilian contexts such as border control and political campaigning, raising serious questions about accountability. Major technology companies and defence startups, such as Palantir, which operates across both spheres, play a central role in eroding the distinction between the military and civilian domains. The panel therefore aims to understand what this convergence means for social rights and broader responsibility, and to explore what civil society advocacy and appropriate safeguards can realistically achieve.

Panellists' contributions

Chantal Joris, Article 19

Joris opened by emphasising that both international human rights law and international humanitarian law apply simultaneously in armed conflict settings, and that technologies such as AI impact a broad range of rights including privacy and freedom of expression. She noted that a certain level of data collection is in fact legally required in order to comply with humanitarian law principles such as distinction and proportionality, as militaries must be able to identify what they are targeting. However, she raised the critical question of whether AI-enhanced data processing genuinely improves compliance or instead undermines it by marginalising human decision-making. She argued that exponential increases in data gathering demand clearer legal limits, stressing that national security does not constitute a blank cheque to override human rights obligations without a proper legal basis, legitimate aim, and proportionality assessment. On accountability, she highlighted the difficulty of attributing responsibility when harm results from systems involving both private companies and state actors. She closed by drawing attention to

the human dimension of mass surveillance, noting that even people in conflict zones retain a legitimate interest in anonymous communication and relationships free from constant monitoring.

Joelle Rizk, ICRC

Rizk joined remotely and opened by stressing that civilian data in armed conflict is not inherently harmful, but that the risks arise from how it is aggregated, processed, and fed into broader infrastructures. She explained that digital surveillance systems and social media platforms can be used to label and track individuals, potentially feeding into targeting systems used in both conflict and law enforcement operations. Crucially, she emphasised that it is not the data alone but the layered civilian infrastructure surrounding it, cloud services, platforms, networks, that enables these harms. She also highlighted a protective dimension: the same data-driven technologies, such as digital battlefield recreations, can function as early warning systems for natural disasters or evacuation tools in humanitarian crises, and may even assist militaries in avoiding civilian harm as a secondary effect. However, she cautioned that much of this data was originally collected in peacetime and for civilian purposes, raising serious ethical concerns about its repurposing. She concluded by noting that humanitarian actors sometimes depend on the same data and infrastructure to fulfil their obligations, painting an overall picture of deep tension between protective and harmful uses of civilian data in conflict settings.

Frank Slijper, PAX

Slijper opened with a historical reminder that technology companies have long collaborated with the military, citing legacy firms such as IBM and Oracle, as well as DARPA's foundational role in developing dual-use technologies including the internet. He traced a key turning point to Project Maven, the US military's effort to use AI to process vast volumes of surveillance data, which Google initially contracted for before withdrawing following intense internal opposition, a moment that produced the first corporate AI ethics policy of its kind. That contract was subsequently taken up by Palantir, and the programme has since evolved into a sophisticated data management and targeting system, reportedly integrated with generative AI and deployed in operations in Venezuela and Iran. Slijper highlighted how the absence of cloud infrastructure a decade ago has given way to multi-billion dollar Pentagon contracts with Google, Microsoft, Oracle and others, making these companies structurally integral to modern military operations, as seen in the use of cloud-based targeting systems in Gaza. He concluded with a pointed political observation: virtually all of these dominant technology companies are American, controlled by an extraordinarily small and wealthy group of individuals who are closely aligned with a US government that has declared AI supremacy over China as a core strategic objective, all while democratic checks on that power are rapidly eroding.

Iverna McGowan, OHCHR

McGowan situated the UN's role as one of monitoring and reporting, supporting special procedures and documenting the real-world human rights impacts of these developments in the field. She reinforced the dual-use concern, noting that the companies at the centre of military AI are the same ones embedded in everyday civilian life, making it structurally difficult to trace where data collected in one context ends up being used. She observed that major governance

frameworks such as the EU AI Act and the Council of Europe Convention have explicitly excluded military applications, leaving a significant regulatory gap given the known dual-use nature of general-purpose AI models. She cautioned against the private sector tendency to assume good faith on the part of actors accessing their systems, noting that field observations do not always bear this out, and described OHCHR's efforts to produce clearer and more concrete guidance to strengthen accountability. She identified a fundamental incompatibility between the rapid pace of AI development and the legal obligations of due diligence and proportionality. Finally, she raised the underappreciated risk posed by physical data centre infrastructure: civilian data is often stored in the same facilities serving military purposes, making those centres potential military targets with catastrophic consequences for civilian populations.

Summary of Q&A discussion

Question 1: Maybe consider a role in providing communication aid from humanitarian aid associations. You accept that in situations of war, civilians will have to use these big tech companies given the dual use, they use Instagram and such, and then their location is gathered and used for war. Are there low-tech solutions to bypass this dual use in wartimes?

Answers:

Rizk acknowledged that safer communication in wartime has been widely discussed but stated plainly that "right now there is no viable option" at scale. She noted that alternative communication strategies carry their own risks, including how states perceive their use and the exposure of individuals to harm as a result. She pointed to grassroots organisations developing such alternatives, or advocating for going offline entirely, but cautioned that adopting this as policy across multiple locations raises serious risks to staff and service users.

Joris described this as a "huge problem" compounded by the enormous market power of a handful of companies who serve everyone simultaneously, creating an inherent conflict of interest. She noted that Iran has arrested and tortured individuals for using Starlink, illustrating the dangers of alternative tools as well. While acknowledging the situation is far from ideal, she argued that solutions must build on existing communication realities rather than ignore them, and called for efforts to decentralise existing systems.

McGowan stressed that end-to-end encryption is protected under human rights law, but warned it is increasingly under threat from states. She emphasised that the issue is not only the lack of availability of secure tools, but the urgent need to protect the underlying norm of privacy itself.

Question 2: On accountability, there are enforcement gaps when it comes to private actors. Can other bodies of law, such as liability frameworks, better hold big tech accountable during wartime?

Answers:

Slijper acknowledged that litigation against companies is "a very new area" with little jurisprudence in the military context but affirmed that anyone connected to a war crime should be held accountable. He noted that while the ICC presents a very high bar, national courts offer a lower threshold, though significant difficulties remain, citing the Microsoft case in Gaza, where

establishing which national legal rules applied to a specific data centre in the Netherlands proved extremely difficult, making it far harder to hold a company to account than a state.

McGowan identified transparency as "a key component to any accountability" and an essential entry point. She called for transparency by design, and where that is absent, for civil society and other vehicles to step in to create the conditions for accountability.

Joris broadened the framing of accountability beyond the legal, pointing to worker protests and whistleblowers as meaningful mechanisms that can mitigate harm. On the ICC specifically, she noted that the Office of the Prosecutor has recently adopted a policy on cyber-enabled crimes, making clear that the commercial nature of an activity does not exempt individuals, including employees of companies, from responsibility for war crimes or genocide. However, she expressed doubt about the ICC's practical effectiveness given its limited resources, noting that cases against companies face even greater obstacles than those against states.

The moderator added that national security is increasingly being deployed alongside commercial interests as a "double barrier" to obscure accountability, calling for more creative use of legal tools in response. She also pointed to the case of ClearView AI, which faced data protection proceedings across multiple Member States while simultaneously pitching its tool to Ukraine, illustrating the paradox of a product built on unlawfully collected data being offered as a solution in conflict settings

Panel Questions

How does AI-driven decision-making reshape compliance with international humanitarian law and international human rights law in practice?

Joris framed the core tension by observing that international humanitarian law and international human rights law apply at the same time in armed conflict, and that a degree of data collection is in fact required for compliance, since a military cannot honour the principles of distinction and proportionality without identifying what it is targeting. The open question, she argued, is whether AI-enhanced processing genuinely improves that compliance or instead erodes it by marginalising human judgement. The moderator had already noted that targeting systems now operate at a speed and scale that strips away meaningful human oversight, and McGowan reinforced the point by identifying a fundamental incompatibility between the pace of AI development and the slower obligations of due diligence and proportionality development. On whether the law itself is adequate the panel divided. Joris resisted the suggestion that the Geneva Conventions and human rights frameworks are outdated, treating the difficulty as one of interpretation and good-faith compliance and stressing that data gathered in peacetime remains subject to human rights law if it is later repurposed for surveillance. Slijper took a different view, contending that the existing laws of war were not designed for the computer age and pointing to the civil-society campaign, now twelve years old, for a binding instrument requiring meaningful human control over all weapons systems, which he suggested might have to travel through the UN General Assembly to bypass the vetoes of Russia, the United States and China.

What surveillance risks do militarised AI techologies pose for civilians during and beyond armed conflict?

Rizk emphasised that civilian data is not inherently harmful and that the risk lies in how it is aggregated, processed and fed into wider systems. Social media and digital surveillance can be used to label and track individuals in ways that feed targeting in both military operations and ordinary law enforcement, and she stressed that it is the layered civilian infrastructure around the data, comprising cloud services, platforms and networks, rather than the data alone that makes such harm possible. She was careful to note a protective side as well, since the same technologies can serve as early-warning or evacuation tools and may even help militaries avoid civilian harm, but she warned that much of the data at issue was gathered in peacetime for civilian purposes, so that its repurposing raises acute ethical problems. Joris drew attention to the human dimension of this monitoring, arguing that people in conflict zones retain a legitimate interest in communicating anonymously and in relationships free from constant observation. McGowan connected the wartime and peacetime risks, noting that the firms at the centre of military AI are the same ones woven into everyday civilian life, which makes it structurally difficult to trace where data collected in one setting is ultimately used, and the moderator observed that tools honed for conflict are readily redeployed in civilian contexts such as border control and political campaigning. McGowan also flagged an underappreciated physical risk: because civilian data is frequently stored in the same facilities that serve military purposes, those data centres may themselves become military targets, with potentially catastrophic consequences for the surrounding population.

What are the responsibilities of tech companies for developing and/or deploying those technologies?

Slijper set the responsibilities of companies against a long history of military collaboration, tracing a turning point to Project Maven, the contract that Google took up and then abandoned under internal pressure, producing an early corporate AI-ethics policy, before it passed to Palantir and grew into a sophisticated targeting system. In his account the leading firms are now structurally integral to military operations through multi-billion-dollar cloud contracts. Nevertheless, a forthcoming PAX study he previewed finds that, while most large technology companies maintain supplier-facing ethical policies, very few govern how their products are used after sale, with Google and Meta weakening their commitments even as Microsoft has tightened its standards under sustained advocacy. McGowan argued that responsibility does not end at the point of sale, cautioning against the industry's tendency to assume good faith on the part of those accessing its systems, insisting that completing due diligence does not absolve a company of continuing obligations. He argues that transparency is the essential precondition for any accountability. Joris located responsibility at the level of individuals as well as firms, pointing to the recent policy of the ICC Office of the Prosecutor on cyber-enabled crimes, under which the commercial character of an activity does not exempt company employees from responsibility for war crimes or genocide, while also highlighting worker protests and whistleblowers as meaningful checks. There was broad agreement that the familiar difficulty, captured in Joris's remark that once a company provides the cloud it can no longer see how the service is used, cannot excuse inaction, and that governments should actively require the firms within their jurisdiction to uphold human rights and humanitarian-law standards.

How can we manage the export of militarised AI technologies into civilian governance and policing?

The panel treated the migration of military AI into civilian governance and policing as one face of a broader erosion of the boundary between the two domains, and did not converge on a single mechanism for managing it. McGowan identified the central regulatory gap in major frameworks such as the EU AI Act and the Council of Europe Convention, which have explicitly excluded military applications. Leaving general-purpose systems of known dual-use only partially governed as it is hard to follow a tool from one setting into another. They gave an illustration of this struggle with ClearView AI. The AI faced data-protection proceedings across several Member States for not complying; nevertheless, it continued to offered its facial-recognition tools to Ukraine. Demonstrating how civilian protections can be circumvented with military exceptionalism. Demonstrating how national security and commercial confidentiality are increasingly used together as a double barrier to accountability. McGowan called for a more creative use of the legal instruments that already exist to combat such exceptionalism. Rizk proposed more concrete safeguards, including reform of procurement policy and explicit guarantees that data collected for humanitarian or civilian purposes is not repurposed for military operations, alongside the possibility of third-party custodians to hold sensitive civilian data, while acknowledging the risk of concentrating such power. Joris and Slijper placed the emphasis on states and norms, with Joris urging governments to require the companies within their jurisdiction to meet human rights and humanitarian-law standards.

Moderator: Ilia Siatitsa, Privacy International - IS

Panellist 1: Chantal Joris, Article 19 - CJ

Panellist 2: Joelle Rizk, International Committee of the Red Cross (ICRC) - JR

Panellist 3: Frank Slijper, PAX - FS

Panellist 4: Iverna McGowan, Office of the United Nations High Commissioner for Human Rights - IM

Rapporteur: Matteo Bard, University of Amsterdam

CPDP 2026
19th international conference

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

Digital Wellbeing, Fairness and Vulnerability

Date: 22 May 2026

Panel Organiser: eLaw Leiden University / RESOCIAL Project

Moderator's Introduction

The moderator opened by introducing the ReSocial Project, a multi-university collaboration including Leiden, TU Delft, Twente, and the Hogeschool of Holland, which departs from the premise that a purely digital society carries significant risks and asks how its opportunities can be captured without those harms. He noted that while much attention has been paid to digital addiction, anxiety, and screen time, social media also plays a genuinely important role in identity formation and socialisation, making outright rejection the wrong framing. He identified the central gap in current law as the absence of a meaningful concept of "digital well-being" and a corresponding harm framework for fundamental rights, arguing that harm must be understood as more than financial or physical damage, a point illustrated by the fact that TikTok's addictive features were fined for their negative consequences rather than for well-being violations as such. Drawing on empirical data from the project, he outlined four features: infinite scroll, autoplay, recommender systems, and push notifications. These are the primary drivers of attention abuse and shortened concentration, a finding now reflected in some litigation in New Mexico and other US states. He closed by highlighting that functional dependency is a key pathway to psychological addiction, with marginalised groups, including those relying on social media to maintain family ties or find community, such as LGBTQ+ youth, disproportionately exposed to its harms.

Panellists' contributions

Helen Vossen, Utrecht University

Vossen opened by noting that the term "addiction" cannot formally be applied to social media in psychological literature (unlike gaming, no official diagnostic category exists). Yet the same behavioural predictors used for poker players and gamers are applied in research. She argued that all adolescents are vulnerable online by definition, as they are still developing and lack both the skills and the motivation to protect themselves, given that social connection is so important to them that they actively ignore warning signs. She highlighted elevated risk for young people with ADHD, who tend toward impulsive oversharing, and for those experiencing depression, who may use social media as a coping mechanism that can either foster peer connection or pull them

into harmful rabbit holes. On media literacy, she was candid that provision is inconsistent and often inadequate, noting that in the Netherlands there is no national curriculum requirement. This leaves schools to decide individuall whether to include media literacy courses, with most defaulting to coding rather than tailored digital literacy education. She identified parenting as a critical protective factor, finding that warmth, engagement, clear screen time rules explained collaboratively with the child, and genuine interest in children's online experiences all reduce risk, though she acknowledged that not all parents have the capacity to provide this without external support from teachers and professionals.

Alexandra Geese, European Parliament

Geese opened by criticising the tendency to reduce the debate to a binary "ban social media yes or no" rather than focusing on concrete solutions, arguing that the DSA already provides tools to embed mental and digital well-being into legal accountability for platforms. She pointed to a telling example in which the Commission challenged TikTok over an addictive update, causing the company to withdraw it, and called on the Commission to apply that same pressure consistently across Instagram, Facebook, and other major platforms. She argued that the Commission's reluctance to do so stems from fear of US political pressure, noting that addictive algorithmic design is treated as protected speech under the First Amendment in the United States, though she noted that even US juries have begun to push back. On education, she urged caution against treating it as a straightforward solution, pointing out that media literacy outcomes correlate strongly with socioeconomic status and that lower-income children with fewer support structures are consistently left behind. She argued forcefully that schools cannot absorb additional requirements without additional funding, and that the cost of addressing harms created by big tech should be met by taxing those companies directly. She closed by reiterating that the goal must be protecting users within social media rather than debating its existence, and that the Commission must stop allowing US commercial interests to dictate the enforcement of European law.

Nina Baranowska, eLaw Leiden University / RESOCIAL Project

Baranowska argued that digital well-being is a multidimensional concept that is genuinely difficult to capture in law, spanning both objective functioning and subjective experience, and noted that while EU law already references well-being, the DSA provides no definition or taxonomy of the harms platforms must address. She proposed a two-element framework for defining digital well-being harm in law. The first element is attention abuse, comprising time exploitation, covering misperception of time spent online and loss of control over it, and problematic exposure, whereby even brief sessions can trigger significant anxiety or distress through intense content. The second element is cascade effects on fundamental rights, in which attention abuse functions as an upstream process leading to deeper downstream harms including mental health impacts such as anxiety and depression, and the commercial steering of user autonomy through design. She stressed that these elements are not the harm itself but the pathway to it, and that law must capture this upstream dynamic rather than focusing solely on visible downstream consequences.

Christos Floros, Monnett

Floros expressed genuine optimism that non-addictive social media is possible, grounding his argument in the structural economics of addiction. He used the cigarette analogy to illustrate that addiction in social media is not incidental but essential to the business model, platforms are built to bring users back repeatedly in order to monetise attention, making the arms race between addictive design and regulation structurally inevitable. He argued that the only viable alternative is to remove the addictive incentive entirely by replacing the attention economy with a subscription model, so that platforms no longer profit from maximising engagement. He acknowledged that persuading users and investors to embrace this model is the central challenge, but described it as the direction his company is actively pursuing. The moderator pushed back gently, suggesting that the cigarette analogy is imperfect given that social media, like sugar, can be both harmful and beneficial, a distinction Floros accepted as worth exploring.

Summary of Q&A discussion

Question 1: Could you, do you think we can find in legal terms what is long-term consumer value? What is fair representation, and as it comes down to what you optimise for, could we use consumer value as an element of regulation?

Answers:

Floros argued that if social media were treated as a product governed by a business model similar to that of traditional media such as newspapers, it would benefit most users. He framed the ideal platform as one that functions like a library, where humans retain agency, see their friends, and nothing more, contrasting this with the current reality in which algorithms strip users of that agency entirely.

Question 2: A better analogy might be food rather than smoking, it can be healthy or unhealthy. To Alexandra: should we not also focus on the app stores? Apple and Google, through their integrated app store environments, have significant leverage, so should we regulate at that level, or even force them to deactivate non-compliant apps?

Answers:

Geese cautioned against giving Apple and Google more power, arguing that regulation should go directly to the app makers rather than routing accountability through the app stores. She stressed the need to distinguish clearly between legal and illegal apps at the source.

Question 3: Young people are not motivated, and media literacy alone may not be enough, will they act in line with what they are taught at school if peer pressure pulls in the opposite direction?

Answers:

Vossen responded that the key is building genuine autonomy by making young people aware that they are not in control on social media, that the platform decides what they see, how long they stay, and what they do. She argued that demonstrating this loss of agency is itself the intervention, as it opens the door to stimulating authentic social connection without platform dependency.

Question 4: In terms of well-being, can we draw lessons from Article 28 guidelines that focus on getting it right? Should we stay with the term social media and focus on how to do it well, not just what to prohibit?

Answers:

Baranowska noted that social media's impact extends beyond consumers to users more broadly, and that fairness is difficult to operationalise as a legal standard. She welcomed the idea of establishing criteria for good practice alongside prohibitions, arguing that showing platforms what they should do, rather than only what they must not do, makes regulation easier to implement and enforce.

Question 5: TikTok is the low-hanging fruit, rather than taxing companies, would it not be easier and less confrontational to partner with them in the name of CSR and simply push for healthier behaviours? And to Alexandra: is heroin not a better analogy than sugar or smoking?

Answers:

Geese warned that working with TikTok to make its algorithm less addictive would simply create space for another company to fill the void, and that regulation is necessary to keep all players in line, describing the free market as "a shark tank." On the analogy, she agreed that heroin or drugs is "definitely much better," pointing to the way major tech companies are using their influence over the US government to block EU legislation such as the Digital Markets Act. She described this as a "drug war move," deploying state power across borders to protect addictive business models, with tech companies effectively capturing state influence through the same structural logic as the drug trade.

Panel Questions

How can we conceptualise digital wellbeing in the EU law, at the intersection of existing tools (Consumer protection acquis, GDPR, AI Act and Digital Services Act) and to inform future law-making, especially the Digital Fairness Act?

The discussion took as its starting point the moderator’s contention that EU law still lacks any meaningful concept of digital well-being and that harm here must be understood as something broader than financial or physical damage. This is a gap he illustrated by bringing forth TikTok’s addictive features and how it had been penalised for their negative consequences rather than for any well-being violation as such. Baranowska developed this into a positive proposal, describing digital well-being as a multidimensional notion that spans both objective functioning and subjective experience and that the existing acquis references without ever defining. She argues that the Digital Services Act provides neither a definition nor a taxonomy of the harms platforms must address, and neither the consumer-protection acquis, data-protection law nor the AI Act fills that gap. A workable conception, she argued, should locate harm upstream in the mechanisms of attention abuse and functional dependency rather than only in its visible downstream effects. The legislation should treat vulnerability as a marker of heightened risk to fundamental rights rather than a fixed attribute of particular groups, and should abandon the habit of describing these services merely as ‘social’, which obscures the addictive architecture

any coherent concept must name. Geese agreed that the Digital Services Act is for now the principal vehicle for holding platforms to account, but was more guarded about what follows: while the Digital Fairness Act offers an opportunity to consolidate these threads into a single accountability framework, she doubted that present majorities in the Parliament and Commission would support a strong text, and warned that the provisions on addictive design most worth having are precisely those most likely to be diluted or displaced by narrower measures focused on minors and biometric data.

How can we operationalise vulnerability-sensitive design for online platforms?

Vossen explained that we are all vulnerable to platforms, it is not unique to certain groups. However, there are certain groups with elevated risks. For example, adolescents are susceptible simply by virtue of their stage of development, with further elevated risk for those with ADHD, who are prone to impulsive oversharing, and for those experiencing depression, who may turn to these platforms as a coping mechanism. If susceptibility is the norm, several speakers agreed, then vulnerability-sensitive design must begin from that assumption rather than treat it as an exception. In practice this means constraining certain traits of social platforms as the moderator presented. These are the infinite scroll, autoplay, recommender-curated feeds and push notifications. Floros located the deeper lever in the business model, contending that genuinely protective design is incompatible with an attention economy and proposing a shift to subscription funding so that platforms no longer profit from maximising engagement, with the aim of a vulnerability-sensitive desings behaving like a library in which users retain agency to select their content and avoid addiction. Vossen complemented this with a broader distribution of responsibility across parents, schools and health professionals, underpinned by an agreed understanding of healthy use and by practical tools accessible even to less digitally literate families, while cautioning that many professionals are themselves inadequately trained. Baranowska pressed the legal dimension, urging that vulnerability be operationalised as a marker of heightened risk to fundamental rights that platforms' design choices are required to take into account. Floros added a caution shared by others, observing that compliance costs fall disproportionately on smaller and newer business, so that operationalising these regulations should not end up smothering smaller business and reinforcing the position of the larger platforms.

Can legal "simplification" efforts coexist with higher protections for human vulnerabilities in the online ecosystem?

The panel did not address simplification directly, and no single position emerged, but the exchange suggested that the two aims can be reconciled only under this question. Floros put the case that streamlining need not be opposed to protection, observing that regulatory complexity and uncertainty weigh most heavily on smaller and newer entrants. He illustrated this point with a personal case where his company needs to fulfill compliance demand from a data-protection authority that his own company lacked the resources to meet, and argued that a clearer and more predictable regime, backed by a genuine EU investment market, would help healthier alternatives raise capital and compete with incumbents. Baranowska offered a complementary thought, suggesting that regulation which specifies what good practice looks like, rather than enumerating prohibitions alone, is easier both to comply with and to enforce, and can therefore be simpler and

more protective at once. Geese was more wary, warning that simplification can serve as a vehicle for weakening rather than clarifying obligations. She saw no current majority for strong legislation and judged that the measures most worth preserving, particularly those on addictive design, are the likeliest to be sacrificed. Taken together, the panel's implicit conclusion was conditional: simplification can coexist with stronger protection where it removes disproportionate burdens on good-faith actors and shifts cost towards the largest platforms, but can be used as a tool to water-down existing and future regluation.

If prohibiting social media to minors is not "the" solution, what might/should we do?

There was broad consensus that prohibition aims at the wrong target. These services support identity formation and social connection; thus, the goal should be to protect users within them rather than to withdraw access completely. The alternatives the speakers offered operated at several levels. At the level of the platforms, Geese argued for holding providers to account for their addictive designs under existing regulatory instruments, like what was done with TikTok, and then applying thaese regulations consistently across all major services rather than selectively. She regarded such design provisions as the single most important measures, even while predicting that a ban for minors and restrictions on biometric data collection were the likelier legislative outcome. At the level of the market, Floros pressed for enabling genuinely non-addictive alternatives through subscription funding and a functioning EU investment market, so that better products can emerge and compete. At the level of the individual and the community, Vossen proposed a model of shared responsibility spanning parents, schools and health professionals. She suggested to support these actors, practical tools, usable by all families should be designed along with training for the many professionals who currently lack it on this subject. Geese cautioned that education cannot carry this burden alone, since media-literacy outcomes track socioeconomic status closely and unfunded reliance on schools risks widening existing inequalities, which is why she maintained that the associated costs should fall on the platforms rather than on strained public budgets.

Moderator: Gianclaudio Malgieri, Leiden University - GM

Panellist 1: Nina Baranowska, eLaw Leiden University / RESOCIAL Project - NB

Panellist 2: Helen Vossen, Utrecht University - HV

Panellist 3: Alexandra Geese, European Parliament - AG

Panellist 4: Christos Floros, Monnett - CF

Rapporteur: Matteo Bard, University of Amsterdam