Brussels Privacy Symposium 2024

Integrating the AI Act in the EU Data Governance Ecosystem

Symposium Report

Authors: Bianca-Ioana Marcu, Vasileios Rovilos, Andreea Şerban

December 2024

FUTURE OF PRIVACY FORUM

The Future of Privacy Forum

In Europe, the Future of Privacy Forum (FPF) is an independent voice, maintaining neutrality in any discourse. FPF is optimistic that social and economic good can be achieved through innovation in data and technology while also respecting privacy and data protection rights. FPF has built strong partnerships across Europe through its convenings and trainings for policymakers and regulators. FPF's transatlantic engagement helps regulators, policymakers, and staff at European Union data protection authorities better understand the technologies at the forefront of data protection law. FPF explains EU data protection and privacy law and the European Court of Human Rights legal framework to make them easily understandable for stakeholders in the U.S. and around the world. FPF hopes to bridge the gap between European and U.S. privacy cultures and build a common data protection language.

A space for debate and dialogue: FPF is a non-profit organization providing a space for debate and dialogue by:

» Sharing knowledge of European privacy and data protection law with its members

» Connecting a network of key players from corporations, NGOs, academics, civil society, and regulators

» Engaging with EU regulatory bodies and policymakers

» Being a respected voice in the media

» Advising corporations and policymakers regarding technological, privacy and data protection issues

» Offering regular peer-to-peer gatherings, workshop, and training interventions in selected hotspots across Europe

Brussels Privacy Hub

At the Brussels Privacy Hub (BPH), we believe strongly in the relevance and importance of data protection and privacy law, particularly in light of the challenges posed by the rapid development of technology and globalization. We also believe that fresh and innovative thinking based on multidisciplinary research is necessary to meet these challenges. The BPH thus brings together scholars from a wide array of disciplines who collaborate with the private sector, policymakers, and NGOs to produce cutting-edge research. We believe in network-building and have built a strong network of contacts with leading privacy researchers both in and outside the EU. The BPH's main goals are to produce privacy research of the highest quality, bring together leading thinkers from around the world, and foster an interchange of ideas among privacy stakeholders in a climate of intellectual openness.

Table of Contents

1. Introduction

The eighth edition of the Brussels Privacy Symposium, co-organized jointly by the Future of Privacy Forum and the Brussels Privacy Hub of the Vrije Universiteit Brussel, took place on Tuesday 8th October 2024 at Les Ateliers des Tanneurs. The Symposium is a multidisciplinary, global convening bringing with it an opportunity to discuss some of the most pressing issues for Europe's digital society today and in the years to come. The theme of this edition built upon conversations held during the 2023 Brussels Privacy Symposium, and focused on **"Integrating the AI Act in the EU Data Governance Ecosystem: Bridging Regulatory Regimes."**

With this year's program, the organizers convened leading stakeholders representing academia, lawmakers, civil society, and industry to spark in-depth, practical discussions on the interaction of the EU's AI law with the GDPR, the Digital Services Act (DSA), and the Digital Markets Act (DMA). Attendees were welcomed by Leiden University's Professor of Law and Technology and co-Director of the Brussels Privacy Hub, Gianclaudio Malgieri, and by Dr. Gabriela Zanfir-Fortuna, Future of Privacy Forum's Vice President for Global Privacy.

In addition to three expert panels, the Symposium opened with a Keynote address by Mark Scott, Senior Resident Fellow at the Atlantic Council, who addressed **"The Digital Challenge for the New Commission,"** noting that the incoming European Commission, in addition to ensuring the effective enforcement of a new generation of digital rules, will also have the task of demonstrating the EU's regulatory response in an era of global competitiveness and technology's intersection with geopolitics. The program also welcomed Dr Lucas Anjos, Postdoctoral Researcher at SciencesPo and Data Protection Specialist in the International Affairs Unit of the Brazilian Data Protection Authority (ANPD) for a Lightning Talk on the **"Brussels Effect" for Global AI Regulation in Brazil** and beyond, as well as Professor Adriana Iamnitchi, Professor and Chair of Computational Social Sciences at Maastricht University, for an Honored Guest Speaker Talk on the **DSA from a Computational Perspective**. Participants had the opportunity to actively participate in three dynamic workshop sessions on topics ranging from children's privacy to whether we should be able to give consent to ChatGPT and tracing the right to explanation from the GDPR to the AI Act. Dr Rob van Eijk, FPF's Managing Director for Europe, and Professor Sophie Stalla-Bourdillon, the Brussels Privacy Hub's co-Director, gave the day's Closing Remarks, sharing their takeaways as well as reflections on the future of data protection.

The following Report outlines some of the most prominent outcomes from the day's conversations, providing summaries and notes of the day's proceedings, starting with the Opening Keynote, and ending with the Closing Reflections from an open dialogue between Prof. Gloria González Fuster, of the Vrije Universiteit Brussel, and Wojciech Wiewiórowski, the European Data Protection Supervisor.

2. Opening Keynote: The Digital Challenge for the New Commission

In the opening of the eighth Brussels Privacy Symposium, **Mark Scott**, Senior Resident Fellow at Atlantic Council, offered a Keynote address reflecting on Europe's digital rules as the incoming European Commission faces challenges in enforcing existing digital regulation and setting a global example in tech governance. Scott highlighted that **the focus must shift from rulemaking to enforcement, requiring strong coordination among European and national regulators**. The Keynote identified the first challenge that the incoming Commission has to confront, which is prioritizing efficient implementation over new legislative developments. Scott addressed the regulation-competitiveness debate, arguing that the current EU rules are not designed to be anti-competitive, and noted that it is up to the European Commission to demonstrate the efficiency of rules on competition and consumer protection while ensuring responsible governance in AI and data protection.

Scott addressed the issue of fragmented enforcement across EU Member States, which is challenged with every new legislative development. He recalled Data Protection Authorities' (DPAs) decades of regulatory experience and suggested a collaborative framework for enforcement providing, as an example, the UK's Digital Regulation Cooperation Forum formed in 2020 to address potential interagency issues.

The second challenge addressed by the Keynote speech concerned the so-called Brussels Effect, recognizing Europe's influence on global digital policy. However, Scott noted a prominent shift: if the EU once led with data protection standards across the world, many countries now view European regulations as overly complex and potentially challenging for economic growth. **This shift challenges the assumption that Europe's lead will be followed, as Scott argued that other global actors such as the US, Brazil, South Korea, South Africa, and Australia are pursuing their own digital frameworks.**

The Keynote similarly emphasized that the incoming European Commission will have the difficult task of demonstrating to the world the benefits of the already-adopted digital rulebook for the EU's global success. It highlighted that the implementation of the DMA, DSA, and the AI Act must showcase stories of success in improving online safety, competition, and innovation. Finally, Scott underlined that the incoming Commission's success will be defined by addressing the challenge of ensuring effective rule implementation and its role at the international level.

3. Unpacking Notions of Risk: From the Data Protection Impact Assessment to Generative AI Systemic Risk and Back Again

The first panel of the Symposium, “Unpacking Notions of Risk: From the Data Protection Impact Assessment to Generative AI Systemic Risk and Back Again,” delved into the concept of risk in the GDPR, the EU AI Act, and the DSA. The discussion, moderated by **Prof. Gianclaudio Malgieri**, aimed at navigating the different notions of risk across EU digital legislation, identifying the risk parameters, what makes a risk “systemic”, and whether and how the same methodology of the DPIA can be leveraged or applied in the context of newer risk assessments. The panel featured Maryant Fernandez Perez, Head of Digital Policy at The European Consumer Organization (BEUC); Dr. Laura Caroli, Senior Fellow of the Wadhwani AI Center at the Center for Strategic and International Studies (CSIS) and Former Senior Policy Advisor at the European Parliament; Lorelien Hoet, Government Affairs Director at Microsoft; and Prof. Niels van Dijk, Associate Professor, Vrije Universiteit Brussel.

3.1 DEFINING “RISKS TO RIGHTS” UNDER THE GDPR

Addressing current definitions of risk, **Prof. Niels van Dijk** suggested that while Court-issued judgments and guidelines have been adopted to date, they still do not articulate what specific “risks to rights” may entail. While DPAs in Germany, France, the UK, and the Netherlands have provided us with guidance on how to assess the concept of “risks to rights”, it nevertheless remains widely debated, especially in light of new challenges put forward by emerging legislation. Van Dijk delved into the concepts of “risks” and “rights,” noting that these come from different background regimes, thus highlighting a critical need to bridge this gap. Drawing from lessons learned, he reflected on types of harm, pointing out that while harm is a central part of the discussion, it is not everything. Van Dijk drew attention to the need for a **more comprehensive perspective on fundamental rights under the GDPR**, which should encompass their function in a constitutional system in which their role is to provide checks to agglomerations of power.

3.2 LEVERAGING LESSONS LEARNED FROM THE DPIA

Answering moderator Malgieri’s question on whether and how we can leverage lessons learned from the GDPR’s DPIA, **Lorelien Hoet** recalled that **the risk-based approach inevitably has an element of proportionality**. She emphasized that its calibration goes hand-in-hand with risk evaluation, identification, and impact assessment, requiring extensive processes and documentation. She noted that while DPIAs are not public, the GDPR and DPAs’ growing interest in them have pushed these instruments to become more robust. Hoet argued that the DPIAs also emphasize potential harm to human rights, as the GDPR’s Article 35 calls for the description of the impact of the intended processing on individuals’ rights and freedoms. She agreed that **the focus on harm has increased over time**, and this is recently seen in the Meta Platforms Inc and Others v Bundeskartellamt judgment (Case C-252/21) and confirmed in the KNLTB v Autoriteit Persoonsgegevens (Case C-621/22) ruling, which required an assessment of the “reasonable expectations” of the data subject. Hoet highlighted an example from the UK ICO on Snap’s DPIA, which pushed Snap to take into account the impact of processing on the data subject. She concluded with a comparison between the DPIA and the DSA impact assessment, the latter of which may be interpreted as prioritizing human rights even more due to its broader and more complex objectives.

3.3 THE CONSUMER RIGHTS' PERSPECTIVE ON IMPACT ASSESSMENTS

To moderator Malgieri's question on how the consumer perspective understands the DPIA, **Maryant Fernández Pérez** stated that it is primarily seen as a tool. She emphasized that there are overlaps between the GDPR, the AI Act, and the DSA, noting that the AI Act's clear intention is to provide some clarifications on using the assessments in a complementary way. Fernández Pérez gave a brief comparison between the three laws, noting that there are differences concerning their scope and objectives, with the DPIA being perhaps narrower and the impact assessment under the DSA being broader. In comparing the three laws, Fernández Pérez also highlighted structural differences, with the DSA covering mainly VLOPs and very large search engines designated as such, and drew attention to a similar approach under the AI Act, depending on whether deployers and providers deal with high-risk AI systems or not.

Fernández Pérez expressed concern over the limited scope of the Fundamental Rights Impact Assessment (FRIA) in the EU AI Act for deployers of high-risk AI systems which, she argued, excludes consumer-relevant areas. She was similarly critical of the AI Act's focus on standardization which may be used as a presumption of compliance for the assessment of fundamental rights, arguing that standardization bodies and their frameworks are not built for consumer interests. Fernández Pérez concluded by underlining the importance of ensuring that risk assessment tools serve people's interests.

3.4 REMEMBERING BEHIND-THE-SCENES AI ACT NEGOTIATIONS TO UNDERSTAND NOTIONS OF RISK

Addressing moderator Malgieri's prompt to recall the lengthy AI Act negotiations, **Dr. Laura Caroli** described the AI Act as primarily a product safety legislation that evolved into a "hybrid" law because of its resemblance to the GDPR. She pointed out key aspects of the AI Act, including a risk management system required for providers of high-risk AI systems. The risk management system provided for in Article 9 of the AI Act is the first of the risk assessments, to be completed by the provider, who needs to assess every type of risk according to the AI system's specific intended purpose.

Caroli **recalled the challenges in expanding the AI Act to include fundamental rights**, noting uncertainties during the AI Act negotiations due to, in part, the negotiating parties' composition of more product safety experts and fewer experts in fundamental rights. She also clarified that the ISO standard 42001, considered to provide a presumption of conformity or almost a close presumption of conformity with the AI Act, does not cover fundamental rights and is incomplete for the purposes of compliance with the law.

With regard to the FRIA, Caroli noted that the focus during negotiations was primarily on Annex III of the AI Act. While it initially faced rejection from the other negotiating parties, Caroli expressed satisfaction that the concept of fundamental rights was pushed through into the final text and that it applies to some of the most sensitive areas, including the use of high-risk AI by public authorities, where the risk of abuse can be high, as well as bank and insurance providers. Lastly, Caroli acknowledged the difficulties during the AI Act negotiations, where product safety and privacy professionals held different perspectives on fundamental rights.

3.5 DISTINGUISHING RISK FROM SYSTEMIC RISK

During the second round of questions, moderator **Malgieri** asked the panel to provide their perspective on the difference between the concepts of "risk" and "systemic risk." **Van Dijk** stated that each risk *could* be systemic, suggesting that **risks have inherently systemic traits**. The legislative concept of systemic risk includes threats to societal functions, civic discourse, and fundamental rights, a shift that elevates rights to a societal level.

Caroli further explained that the notion of systemic risk in the EU AI Act applies to General Purpose AI (GPAI) models, which is broader than Generative AI only, stating that the concept of systemic risk in this context has been drawn from international standards. **Fernández Pérez** addressed the interplay between the two notions of systemic risk in the DSA and the AI Act, recalling that while the DSA does not provide a clear definition yet, it does provide some guidance which will develop over time. Lastly, **Hoet** focused on how companies such as Microsoft are adapting to these frameworks. She noted that many companies already have ethical frameworks in place that provide a solid basis for risk assessment and mitigation. She also described an internal governance model to address the overlapping requirements of the GDPR, the DSA, and the AI Act.

4. Lightning Talk — The Brussels Effect in Global AI Regulation: Reflections from Brazil

During his Lightning Talk, **Dr. Lucas Anjos,** Postdoctoral Researcher at the SciencesPo School of Law and Data Protection Specialist at the International Affairs Unit of the Brazilian Data Protection Authority (ANPD), explored the emerging framework for AI regulation in Brazil, providing a comparison with the EU's approach in light of the "Brussels Effect." This concept relates to how the EU's regulatory standards influence other jurisdictions globally, including Brazil, which has modeled many aspects of its legislative frameworks on European laws, particularly in the field of digital policy. Anjos, however, emphasized important nuances between the two approaches, discussing both convergences and divergences in the regulatory landscape.

The Brazilian AI Bill, currently under discussion in the Brazilian Congress, is a work in progress but demonstrates clear parallels with the EU's AI Act. It adopts a risk-based, asymmetrical regulatory approach similar to the European model, which seeks to balance innovation with necessary safeguards. Anjos noted that the Bill aims to harmonize standards, definitions, and concepts across sectors while maintaining flexibility for sectoral regulations, particularly in areas like market surveillance. This reflects a key principle of proportionality that characterizes technology regulation globally, including in the EU's DSA and DMA. Despite these similarities, the speaker noted that Brazil's federalist structure introduces unique challenges in implementing centralized regulatory frameworks.

One of the primary convergences between the Brazilian and European approaches is the focus on calibrating AI regulation to address risks while fostering innovation. In Brazil, like in the EU, there is robust debate among legislators, academics, civil society, and the private sector regarding the perceived trade-offs between regulation and innovation. Anjos pointed out that Brazil's legislative discussions reflect many of the same concerns as those in the EU, particularly regarding competitiveness and responsible innovation. However, the Brazilian context presents additional challenges given the country's economic and technological disparities. **Brazil's AI sector, for instance, is largely focused on second-layer applications rather than foundational AI development**, and its investment capacity is significantly lower than that of the EU.

Divergences between the two jurisdictions are equally notable. One key difference highlighted by Anjos is the Brazilian legislature's hesitance to predefine categories of prohibited or unacceptable risks in AI use. While the EU AI Act explicitly categorizes certain uses of AI as prohibited, Brazil has adopted a more pragmatic and less prescriptive stance. Although public and civil society pressure has pushed for stricter prohibitions, particularly concerning high-risk applications like autonomous weapons, the Brazilian legislative process has been slower to impose such constraints. Anjos noted that **this evolving approach could pose challenges for future interoperability between AI regulations across different jurisdictions**, especially if other countries adopt more stringent lists of prohibited AI uses.

The speaker also emphasized the role of civil society in shaping AI regulation in Brazil, describing a process of "tropicalization," where international standards are adapted to fit the local context. Anjos noted that Brazil's strong tradition of civil society engagement in legislative processes has led to

ensuring that AI governance frameworks in Brazil emphasize democratic participation and human rights, distinguishing it somewhat from other regulatory models.
Anjos explained that economic considerations play a significant role in Brazil's AI regulation, particularly given the country's developing market. **While competitiveness is a concern in the EU, it is an even greater challenge for countries like Brazil**, where issues such as digital infrastructure and connectivity are ongoing problems. Legislators must account for these structural challenges when designing AI regulation, and this has led to a more flexible, market-oriented approach compared to the EU.

Looking ahead, Anjos anticipated significant challenges in ensuring interoperability between AI regulations in different countries. Unlike data protection, which has seen broad global convergence, AI regulation could become more fragmented due to differing risk assessments and economic conditions. However, he believes the "Brussels effect" remains strong, as Brazil continues to look to the EU for regulatory inspiration while also incorporating global perspectives from countries like Canada, Chile, and recommendations from the OECD and UNESCO.

In his conclusion, Anjos suggested that while there are important divergences in Brazil's AI regulatory approach, the influence of the EU remains significant. As Brazil's legislative process continues to evolve, the country is striving to balance economic realities with a rights-based approach to regulation, navigating the complex intersection of innovation, governance, and global standards.

5. The Sensitive Personal Data Spectrum: From Positive Obligations to Prohibitions

The second panel of the Symposium discussed the complex interplay between the AI Act, DSA, and GDPR in regulating the processing of sensitive personal data. It explored the prohibitions and obligations imposed on various actors, particularly in the context of advertising and high-risk AI systems. The panel also delved into the challenges of balancing these requirements and ensuring that data protection is maintained while enabling innovation. **The central theme revolves around the dual nature of sensitive personal data — how it can serve both as a shield to protect vulnerable communities and a sword to combat systemic bias and discrimination.** The Panel featured Emerald de Leeuw-Goggin, Global Head of Privacy and AI Governance at Logitech; Lex Zard, Technology and Human Rights Fellow at Harvard Carr Center for Human Rights; Kim Smouter-Umans, Executive Director at European Network Against Racism (ENAR) and was moderated by Michael van den Poel, Research Engineer at EDHEC Business School.

The moderator, **Michael van den Poel**, opened by framing the discussion around sensitive personal data, a concept that has been central to data protection for over two decades. He highlighted the growing complexity of this issue as new EU legislation, such as the DSA and AI Act, introduced different treatments of sensitive data, from prohibitions in targeted advertising to allowances for debiasing AI systems.

5.1 SENSITIVE PERSONAL DATA PROCESSING AS A DOUBLE-EDGED SWORD

Kim Smouter-Umans provided a critical perspective on the origins and intent behind the GDPR's sensitive data provisions. He underscored that these protections were instituted to prevent the misuse of certain types of data, particularly for historically marginalized communities. Smouter-Umans also pointed out that **sensitive data acts as a safeguard against discrimination and harmful outcomes**, such as the misuse of data in the Holocaust and, more recently, in the Netherlands' social services scandal. He emphasized that GDPR provisions are intended to recognize the power imbalance between data controllers and individuals, especially vulnerable communities. However, he also noted a misinterpretation among some entities that the GDPR prohibits the collection of sensitive data outright. Instead, the GDPR sets additional safeguards to manage higher risks associated with the processing of such data.

Smouter-Umans further argued that sensitive data could be a "sword" to combat discrimination, enabling civil society to effectively diagnose and address systemic biases. The lack of such data, he said, often hampers efforts to detect and challenge discrimination across Europe. He advocated for the collection of sensitive data, provided it is done responsibly, as a necessary tool for advancing racial equality and addressing structural injustice.

5.2 TENSION AND CONVERGENCE BETWEEN THE DSA AND AI ACT ON SENSITIVE DATA

Lex Zard, as a DSA expert, shifted the focus to the DSA's provisions on sensitive personal data. He explained that the DSA prohibits the use of sensitive data for targeted advertising to prevent manipulation, disinformation, and discrimination. Zard outlined how behavioral advertising — specifically surveillance advertising based on personal data — can exploit users' vulnerabilities, which the DSA aims to address. He traced the legislative background, revealing that the original proposal lacked a ban on behavioral advertising, but pressure from the European Parliament and civil society resulted in a compromise that limits targeted advertising based on sensitive characteristics.

Zard added that this prohibition aligns with industry standards already adopted by companies like Meta and Alphabet, which have voluntarily ceased targeting based on certain sensitive characteristics since 2021. However, he warned of **potential legal challenges in defining and interpreting sensitive data under the DSA**, especially in light of recent court decisions. Zard concluded that while the DSA seeks to strike a balance between regulating and allowing certain advertising models, enforcement challenges will likely arise, and unintended consequences may affect smaller companies.

Smouter-Umans then returned to address the AI Act, specifically its allowance for using sensitive data to "de-bias" high-risk AI systems. While he welcomed this provision as a step toward mitigating discrimination in AI, **he stressed the need for civil society involvement in AI design and deployment to ensure that the debiasing process reflects the perspectives of affected communities**. Smouter-Umans raised concerns about the systemic biases ingrained in society and, consequently, in datasets used to train AI systems. Without proper oversight, AI could amplify these biases rather than mitigate them.

5.3 OPERATIONALIZING DATA PROTECTION AND AI GOVERNANCE PRINCIPLES TO PROTECT SENSITIVE PERSONAL DATA

Finally, the discussion turned to practical challenges in implementing the complex web of regulations. **Emerald de Leeuw-Goggin** provided an insider's perspective on operationalizing data protection compliance in light of new AI governance requirements. She argued that **privacy professionals are well-positioned to lead AI governance efforts**, as many of the challenges in AI — such as fairness, accountability, and transparency — are rooted in familiar data protection principles. De Leeuw-Goggin suggested leveraging existing privacy frameworks and operational processes to meet the new legal obligations under the AI Act, rather than reinventing the wheel.

Both Smouter-Umans and de Leeuw-Goggin delved into the challenges and necessary actions regarding data collection, fairness, governance, and the role of civil society, particularly in the context of AI regulation. Smouter-Umans stressed the importance of equality in data to better understand disparities, such as in healthcare access, calling for more supportive regulatory signals to encourage the collection of such data. The discussion also emphasized the need for transparency in how companies use this information, advocating for informed consent, particularly from vulnerable communities. Smouter-Umans highlighted that civil society organizations play a vital role in identifying risks but often lack the resources and capacity to raise awareness about their important advisory role in the ecosystem. He urged for better funding mechanisms and insisted that impact assessments should be more public to foster accountability.

De Leeuw-Goggin added that **privacy and fairness are non-negotiable in technology and AI governance**. She underscored the overlap between data protection policies and AI governance but advised moving away from a trade-off mentality between privacy and innovation. Instead, organizations should aim for both, ensuring fairness by processing sensitive data when necessary to meet legal and moral obligations. De Leeuw-Goggin also highlighted that existing processes can be adapted for AI compliance, emphasizing the importance of practical, compliant procedures that are scalable and effective.

The panel agreed that greater engagement with communities, resourcing, and transparency will be essential moving forward, ensuring that vulnerable populations understand their rights and the risks associated with their data. The discussion underscored the complexity of balancing sensitive data protections with efforts to combat bias and discrimination, particularly in the evolving landscapes of digital advertising and AI. While sensitive data can both protect vulnerable communities and be used to challenge systemic injustice, its misuse can lead to significant harm. The challenge ahead lies in ensuring that new regulations like the DSA and AI Act are effectively implemented and enforced, without undermining the GDPR’s foundational protections.

6. Honored Guest Speaker Talk: Bits on the Digital Services Act from a Computational Perspective

For the eighth edition of the Brussels Privacy Symposium, the organizers introduced the Honored Guest Speaker Talk as a feature of the program which connects prominent disciplines, such as social and computational sciences, to data protection and digital policy. This year, we welcomed **Prof. Adriana Iamnitchi**, Professor and Chair of Computational Social Sciences at Maastricht University, as the honored guest speaker, who discussed her work in computational social science. Prof. Iamnitchi's research focuses on data that is generated through the "digital crumbs" left by users on various online platforms. Her work focuses on analyzing social issues through social media data. One aspect of her research focuses on disinformation, and in her speech, Iamnitchi used the case of the Syrian organization "the White Helmets" to illustrate how disinformation operates online, often supported by state-run or conspiratorial channels, and how such campaigns are amplified on social media platforms. Her research focused on collecting social media data and analyzing patterns to detect disinformation networks.

Prof. Iamnitchi emphasized the challenge of replicating studies in computational social science, arguing that data is often inaccessible or subject to change due to platform policies. Prof. Iamnitchi underlined the DSA's impact on researcher access to and use of data, particularly Article 40, which provides for data access and scrutiny, and would give researchers access to social media data for studying platform moderation practices. Together with her team, Prof. Iamnitchi analyzed the DSA transparency database to evaluate how platforms report content moderation practices and compliance with the regulation. Their evaluation showed that platforms often avoid detailed reporting. The speaker further exemplified that Google Shopping was the highest reporter of violations, and X reported minimal moderation activity, having only the non-automated detection of what was wrong, raising questions about the "human factor" role in the decision-making process. The research showed that the reason for moderation is based on illegal content or terms of service. In this sense, Prof. Iamnitchi highlighted that most of the reporting is based on the terms of service of the platform, this being the platform's preferred option.

The research further shows that few platforms report on language-based moderation despite the transparency database offering this as an option. Also, platforms often cite broad terms and conditions, providing little clarity regarding violations. Prof. Iamnitchi noted that terms of service continue to be preferred to legal interpretation. Prof. Iamnitchi concluded by connecting these issues to elections, noting different disinformation practices worldwide adapted to the specificities of the concerned countries. Finally, she questioned the privacy laws and to whom they are applicable when data that could further understand "bad players" is protected.

7. Regulatory Perspectives and AI Enforcement — A Case of Double Jeopardy?

The final panel of the Symposium focused on the complex enforcement landscape under the EU digital rulebook, where several national and regional authorities aim to cooperate effectively in order to avoid a case of "double jeopardy". The panel noted that the recently established AI Office, under the auspices of the European Commission, will play a key role in the implementation of the AI Act, particularly with regard to General Purpose AI. At the same time, over the past two years, DPAs have taken action against providers of AI systems on the basis of the GDPR and, in some jurisdictions, have included the supervision of AI systems in their current and future strategies. Similarly, standardization bodies are tasked with translating the AI Act's technical requirements and obligations into implementable standards for compliance with the law. The panel featured Yordanka Ivanova, Legal and Policy Officer, AI Regulation and Compliance team at the AI Office; Sven Stevenson, Director of Coordination and Supervision on Algorithms at the Dutch DPA; Chiara Giovannini, Deputy Director-General and Senior Manager for Policy and Innovation at ANEC, the European Consumer Voice in Standardisation; Thiago Moraes, Coordinator of Innovation and Research at the Brazilian DPA; and was moderated by Bianca-Ioana Marcu, Deputy Director for Global Privacy at the Future of Privacy Forum.

7.1 ZOOMING IN ON THE ROLE OF THE AI OFFICE IN THE AI ACT'S SUPERVISION AND ENFORCEMENT ARCHITECTURE

To start the conversation, moderator **Bianca-Ioana Marcu** noted that our primary role for the time being is to better understand the architecture of AI Act enforcement. In doing so, two crucial features emerge: the first relates to the fact that there are different roles assigned to different actors within the enforcement architecture, with the AI Office as a central structure; and the second highlights the development of alternative regulatory models introduced by the AI Act, such as codes of practice, self-reporting, standards, sandboxes, and conformity assessments. With this context in mind, **Yordanka Ivanova** noted that the success of the AI Act lies in the framework for its implementation, which the AI Office is tasked with developing.

To give a practical example of this framework, an important element is to specify the rules on General Purpose AI (GPAI) models. Ivanova highlighted that after public consultations and an inclusive plenary process with more than 1,000 stakeholders, the drafting of the Code of Practice for GPAI models is underway. This instrument will be crucial in further detailing the high-level obligations for GPAI models under the AI Act. Ivanova noted that similarly important provisions relate to prohibited AI systems, applicable as of February 2025, for which the AI Office is developing implementation guidelines with practical examples to help both providers and competent authorities in dealing with different applications of prohibited AI systems.

Ivanova added that similarly important implementation and enforcement tools include standards developed by European standardization bodies, as well as regulatory sandboxes. Active engagement with AI systems providers will be crucial in the success of these regulatory tools, as demonstrated by the AI Pact through which companies agree to already implement key AI Act provisions before the deadlines start to apply. In this sense, Ivanova noted that the AI Office has received concrete commitments from big players like Google, IBM, and OpenAI, among others, as well as from small companies that want to prepare for implementation. Together with the AI Office, the AI Board will help EU Member States establish their own competent authorities to ensure overall EU coordination on enforcement.

To prepare for its role as enforcer of the rules on GPAI models, Ivanova highlighted that the AI Office is building its technical capacities by establishing the technical infrastructure necessary for enforcement and by hiring the right experts to support these tasks. Crucially, Ivanova stated that the role of the AI Office is also to ensure overall consistency with all Commission priorities and policy initiatives, with a focus on coordinating AI policy integration into other policy areas and supporting AI innovation and research.

7.2 PRESUMPTION OF CONFORMITY: ALL EYES ON STANDARDS

Moderator Marcu turned to **Chiara Giovannini** to expand upon the precise role and scope of standards in the context of AI Act compliance. Giovannini highlighted that, fundamentally, standards are going to be used to provide a presumption of conformity for high-risk AI systems. Under Article 40 of the AI Act, the European Commission has requested the development of such standards, which is a legislative technique that is also used more generally in EU product safety legislation. Standardization bodies already work on standards in other areas such as on the safety of toys, fridges, computers, and mobile phones, and are therefore well-versed in developing safety rules.

Giovannini noted that currently, much of the pre-standardization work is underway, with the final standards expected to be ready by April 2025. However, Giovannini also warned that they are still quite far away from this deadline because of a laborious process for cooperating and finding agreement on language. She noted that **while standardization is an open process, the stakeholders that have the most to gain are the ones that are able to invest the most resources**. Giovannini asked the audience to think about the legal effect of providing a presumption of conformity and to imagine which stakeholders stand to gain the most from participating in standardization.

Giovannini further explained that, in simple terms, “standards with legal effect” means that an economic operator putting a product on the EU market can certify that the product is following the given standards and is thus presumed to be compliant with all of the requirements of Section 2 of the AI Act. It is then up to the designated market authorities to prove non-compliance, placing us in the presence of a **reversal of the burden of proof**. Giovannini noted that while standards with legal effect are a very important regulatory tool, the challenges presented by AI technologies are novel and complex. She therefore closes her first intervention by asking the audience: Can we rely on standards for AI in the same way that we are used to relying on standards that set the safe temperature for your fridge?

7.3 DATA PROTECTION AUTHORITIES TAKE ACTION

Moderator Marcu turned to **Sven Stevenson** to describe the Dutch DPA's approach to AI supervisory policy, and where DPAs may play an important role in the enforcement of the AI Act. Stevenson noted that it is first and foremost important to distinguish the DPA as a broader organization from the DPA as the supervisor of the GDPR. He highlighted that a DPA's role as a market surveillance authority under the AI Act is completely different from its role as GDPR supervisor and enforcer. In the Netherlands, the DPA has the luxury that since last year, it received additional funding and was requested to take an additional role as a coordinating authority when it comes to AI and algorithm supervision. For the Dutch DPA, this was a very natural basis from which to start preparing, with all other supervisors in the Netherlands, for the AI Act. Stevenson noted, however, that for the DPA as an organization, this means building up and understanding a regulatory framework that is completely different from the GDPR. **AI Act supervision does touch on the same topics as GDPR enforcement but deals with different dynamics and mechanisms.**

Stevenson added that, for example, if serious incidents occur as a result of the deployment of an AI system that is in the scope of the "high-risk" category, it may also present significant GDPR-related issues. Attention will have to be given to ensure cooperation between the different actors, which is why the Dutch DPA is investing as much as possible in understanding this new type of regulatory framework and participating actively in it.

7.4 FROM DATA PROTECTION TO AI REGULATION: THE CASE OF BRAZIL

Moderator Marcu turned to **Thiago Moraes** to add a global perspective to the panel and share how the ANPD, Brazil's DPA, is approaching AI supervision on the basis of Brazil's own data protection law, the LGPD. Moraes noted that Brazil's data protection law has many similarities to the GDPR, one of them being the clause on automated decision-making which clearly relates to how AI systems may operate. Brazil's DPA is therefore aiming to develop descriptive norms and a guideline on this topic, gathering learnings gained from the **"test and learn" approach** taken with the introduction of a regulatory sandbox for AI.

Launched in 2022, the regulatory sandbox exercise allowed the Brazilian DPA to conduct benchmarking with other DPAs, including from Europe, Singapore, and Colombia, and to carry out a public consultation on AI and data protection. Moraes highlighted that, for now, the goal from the DPA perspective is to tackle the discussion on algorithmic transparency and what this might mean in practice, particularly in the context of the country's data protection law.

At the same time, the Brazilian DPA is also dealing with some enforcement cases. For example, the Brazilian DPA led an enforcement case related to Meta and its collection of personal data to train AI without being transparent, which led to the temporary suspension of this type of processing in Brazil in July 2024. Following the suspension, Moraes explained, Meta shared with the DPA their plan to develop more transparency mechanisms for personal data processing for AI training. For more, consider FPF's detailed overview of this case: Processing of Personal Data for AI Training in Brazil: Takeaways from ANPD's Preliminary Decisions in the Meta Case, by Maria Badillo, Policy Counsel for Global Privacy.

7.5 FROM NATIONAL TO REGIONAL COOPERATION

Elaborating on the different national-level authorities tasked with supervising and enforcing the AI Act, **Stevenson** noted that different perspectives from different domains will be crucial, as will the infrastructure for cooperation. **Ivanova** noted that the AI Act does indeed provide flexibility and procedural autonomy to EU Member States to decide how to set up their enforcement mechanisms, depending on their resources. Even in cases where enforcement will be centralized, Ivanova stresses that the AI Act still requires very close collaboration with fundamental rights authorities. **Giovannini** added that from the consumer perspective, the goal is to have standards that we can trust for protecting consumers and society, which is difficult and delicate. The discussion is currently focused on health, safety, and fundamental rights, elaborating on which fundamental rights are at risk and how to benchmark possible standards. **Moraes** noted that while the conversation on the AI Bill in Brazil is still ongoing, the need for cooperation and coordination is also clear in Brazil when it comes to enforcement. There will be a proposal for a national system for AI regulation governance with a central AI authority, which hopefully might be the Brazilian DPA, which may then have the task of dealing with all other sectoral regulators in the country. One thing remains clear when it comes to AI enforcement: regulatory cooperation will be crucial to its success.

8. Closing Reflections: In Conversation with Wojciech Wiewiórowski and Prof. Dr. Gloria González Fuster

This year's Closing Reflections between **Prof. Gloria González Fuster**, of the Vrije Universiteit Brussel, and **Wojciech Wiewiórowski**, the European Data Protection Supervisor, explored the current and future challenges posed by AI, especially from a European perspective. Their dialogue touched upon the broader regulatory landscape shaped by various legislative instruments such as the GDPR, the AI Act, the DSA, and the Data Governance Act. The conversation centered on AI regulation, its intersections with data protection, and the ongoing complexities in shaping a cohesive framework for regulating emerging technologies.

Prof. González Fuster opened by expressing a sense of optimism, asking the Supervisor whether he shared this sentiment, particularly in relation to Europe's trajectory with AI regulation. Supervisor Wiewiórowski acknowledged that while there are considerable challenges ahead, Europe is on the right path. He emphasized that these challenges are not problems *per se* but hurdles that need to be overcome with an open-minded approach. Though optimistic about the overall strategy, he was cautious at first, recognizing that Europe does not yet have all the answers to the complexities of AI regulation.

Supervisor Wiewiórowski further pointed out that Europe's approach to AI must be globally coordinated, given that AI tools and systems are used globally. This makes international cooperation a necessity, not just an option. In contrast to data protection, where cultural differences shape different approaches to privacy, AI demands a more unified, global response since the technology and its impacts transcend borders.

A significant part of the conversation revolved around the AI Act and its place within Europe's broader regulatory ecosystem. Prof. González Fuster and Supervisor Wiewiórowski noted that the AI Act aims to introduce a risk-based framework for AI systems, categorizing them into different risk levels. Initially, the Supervisor was skeptical about the added value of the AI Act, but over time, he came to appreciate its importance in structuring a regulatory approach that balances innovation with fundamental rights protection. Moreover, he pointed out that the AI Act presents a particular challenge for DPAs as it introduces new responsibilities, including market surveillance.

Supervisor Wiewiórowski highlighted that the EDPS and other national DPAs face unique challenges in this space. While the EDPS's oversight of AI within EU institutions might be relatively straightforward, the national DPAs will need to grapple with a more complex reality. They will have to collaborate with other regulatory authorities responsible for AI, **given that AI regulation does not solely pertain to data protection but touches upon market dynamics, consumer protection, and fundamental rights**. The lack of clear roles for DPAs in AI enforcement at this stage was noted as a concern, suggesting that clearer coordination will be required moving forward.
Prof. González Fuster raised the issue of risk, noting the complicated and sometimes contentious understanding of risk in different regulatory instruments, including GDPR. Supervisor Wiewiórowski responded by agreeing that the term "risk" can be a false friend in regulatory contexts, as it is understood differently across various frameworks. He noted that the GDPR's risk-based approach,

where organizations assess data processing risks to privacy, differs from the AI Act's approach to assessing risks based on the potential harm of AI systems. This divergence in the conception of risk adds complexity to how different regulatory instruments will interact with one another.

Supervisor Wiewiórowski praised the work done by European institutions in advancing the AI Act but underscored that more clarity is needed, particularly in the definitions of terms like "market surveillance" in relation to AI. This ambiguity needs to be resolved for effective implementation.

Another key theme of the discussion was the tension between innovation and regulation. Supervisor Wiewiórowski acknowledged that while regulation can sometimes stifle innovation, it is necessary to ensure that technological developments align with societal values, particularly fundamental rights. **He dismissed the often-repeated argument that regulation inherently blocks innovation, pointing out that the role of regulators is to strike a balance that allows innovation to thrive while ensuring safety and ethical standards.** This balancing act is central to Europe's approach to AI and other emerging technologies.

Supervisor Wiewiórowski also shared his personal experience from the 1990s, where early data mining practices that were once deemed innovative later became subject to regulation under new data protection laws. This evolution, he noted, is a natural part of technological progress and regulation.

In discussing other regulatory frameworks, Supervisor Wiewiórowski expressed skepticism about the real impact of the Data Governance Act. He acknowledged that while it is a binding law, its role in shaping data governance in Europe is unclear, and its practical implementation may not be as influential as initially hoped. Similarly, the Data Act, while also significant, presents challenges in creating a comprehensive approach to data processing.

Prof. González Fuster and Supervisor Wiewiórowski concluded by **emphasizing the importance of education and public awareness in ensuring that AI and data governance frameworks are understood not only by regulators and companies but also by the general public**. The Supervisor noted that the ultimate aim is to protect people, not just data. The importance of transparency and ensuring that individuals understand how their data and interactions with AI are governed was underscored as a critical part of future regulatory efforts.

While optimistic about the path ahead, Supervisor Wiewiórowski acknowledged that much work remains, particularly in coordinating global efforts and ensuring that regulatory frameworks like the AI Act and GDPR work together harmoniously. The discussion underscored the delicate balance regulators must strike between enabling innovation and safeguarding fundamental rights, a challenge that will continue to shape the future of AI governance.

9. Thank You and Acknowledgements

The Future of Privacy Forum and the Brussels Privacy Hub, as co-organizers of the eighth edition of the Brussels Privacy Symposium, would like to thank **all of the speakers and attendees for their active and meaningful participation** in the day's proceedings. We would like to share a special note of appreciation and acknowledgment for those joining the Symposium from far and wide, beyond the Brussels borders, including from the U.S., Singapore, and many more.

The organizers extend a warm thank you to the co-facilitators of the Workshop Sessions: Dr. Ingrida Milkaité (Ghent University) and Kay Vasey (k-ID) for leading the workshop on **"Safe Play: designing privacy friendly and age-appropriate digital playgrounds for tomorrow's gamers;"** Vincenzo Tiani (Vrije Universiteit Brussel & Panetta) and Andreea Şerban (FPF) for leading the workshop on **"The right to explanation across the GDPR and AI Act;"** and to Bárbara Lazarotto (VUB) and Pablo Trigo Kramcsák (VUB) for leading the workshop on **"Should we give consent to ChatGPT?"**

We would also like to similarly share a warm thank you to this year's sponsors: **Microsoft**, **k-ID**, and **Wilson Sonsini**, for providing us with the lunch and coffee breaks that are important moments for everyone to connect throughout the day.

Last but certainly not least, we thank **all of the staff of the Future and Privacy Forum and the Brussels Privacy Hub** for their brilliant ideas, efforts, patience, and positivity that went into building this year's program. Thank you to the excellent A/V crew that kept the day running smoothly.

We look forward to welcoming you again for the Brussels Privacy Symposium 2025!

FUTURE OF PRIVACY FORUM

1350 Eye Street NW, Suite 350, Washington, DC 20005
Avenue Marnix 13-17, 1000 Brussels, Belgium

fpf.org