Symposium on AI and Digital Regulation:

Impact on Human Rights and Freedom of Expression

On March 19, 2024, The Future of Free Speech and the Center for Democracy and Technology, Europe Office, brought together leading voices from civil society, EU institutions, and the private sector to discuss the implications of the new wave of EU digital regulation for human rights and freedom of expression. The symposium consisted of three panels.

This document, prepared by The Future of Free Speech, summarizes the key takeaways from the symposium discussions. For a more complete account, please watch the symposium recordings.

Panel 1: The AI Act: Implications for Human Rights

The first panel was moderated by Laura Lazaro Cabrera – Counsel and Director of the Equity and Data Programme at the Center for Democracy and Technology, Europe Office – and explored the realities of drafting and passing the AI Act, civil society's human rights concerns, and how the industry has interacted with the landmark legislation.

Lidiya Simova – Political Advisor to MEP Petar Vitanov – talked about the AI Act adoption process. Starting in April 2021, the bill went through many amendments before it was finally approved in January 2024. The Act is a complex piece of legislation that covers many topics and areas of expertise. While the AI Act was proposed as a product safety law, Simova pointed out that AI is not just like any other product, given the impact it may have on its users. AI also has implications regarding personal data and may be used in law enforcement and the judiciary, affecting important citizens' rights. All these considerations made the AI Act a complex file that generated difficult questions and tradeoffs. Simova also reflected on the time pressure EU institutions faced, given the fast-paced nature of AI technology, and the desire to have future-proof legislation. Given that the initial AI Act proposal focused on single-use AI, the AI Act also had to be adjusted to include general-purpose systems. Simova also mentioned significant lobbying from interest groups and EU member states during the adoption process. She also stressed that when it comes to using biometric identification technologies, the AI Act establishes protections that are at least as robust, if not more, than prior EU legislation.

Connor Dunlop – European Public Policy Lead at the Ada Lovelace Institute – highlighted that while the AI Act has some shortcomings, it is positive that the EU has a higher degree of protection than

any other jurisdiction. Speaking of prohibited AI uses, civil society has concerns regarding the exemption that allows the use of remote biometric identification in certain instances. As a result of pressure from EU member states, this exemption is quite broad, potentially putting citizens' rights at risk. Regarding high-risk AI uses, Dunlop regretted that the AI Act did not adopt a precautionary approach – this approach would have resulted in any AI system being used in a high-risk area being considered high risk and, hence, subject to strict obligations. The current AI Act approach seems to allow companies to self-select and determine whether their AI use is high-risk or not. Regarding general-purpose systems, Dunlop pointed out that there had already been discussions on how to regulate this technology before ChatGPT came out. Ada Lovelace Institute was happy to see general-purpose systems were regulated in the AI Act despite lobbying, including by governments, pushing for the contrary. Dunlop highlighted that it is important to pay attention to the future codes of practice that operationalize the AI Act as there is the risk that they could become very industry-driven. The Ada Lovelace Institute was also happy to see centralized enforcement with the AI office.

Richard Wingfield – Director, Technology Sectors, at BSR – shared an industry perspective of the AI Act, recognizing that many different views exist across and even within companies. Wingfield highlighted that companies within and outside the EU have been closely following the AI Act, given that it can become a global standard. Initially, a key question for the industry was understanding the goal of the AI Act, whether it was product safety, the protection of human rights, or others. Currently, there are concerns regarding the lack of clarity in the regulation, including what uses of AI are prohibited. The convoluted language in the Act likely comes from the tension between the need for comprehensive future-proof legislation and the rapidly evolving AI technology. Wingfield also pointed out that it is likely positive that the EU was the first to regulate AI, given the importance that this jurisdiction grants to fundamental rights. Ultimately, he says, businesses "cautiously welcome" the AI Act. A lot will depend on how it is implemented, which is still unknown. Wingfield argued for a collaborative and constructive approach between public authorities and businesses regarding the AI Act's implementation, with companies able to adapt and learn over time.

Panel 2: What Does the DSA Mean for Freedom of Expression?

The second panel was moderated by Jordi Calvet-Bademunt – Research Fellow at The Future of Free Speech – and focused on what the Digital Services Act means for freedom of expression and online safety.

Asha Allen – Advocacy Director for Europe, Online Expression & Civic Space at the Center for Democracy and Technology, Europe Office – pointed out that much remains to be seen on what the Digital Services Act (DSA) does right or wrong. Allen, however, considered the DSA to be a good starting point. She referred to the DSA's two-pronged approach with clear, concrete obligations on how to tackle illegal content and mandatory due diligence obligations. She also praised the system of tiered obligations imposed on companies depending on the type of services they provide, their size, and the importance the DSA grants to human rights. Allen expressed that the DSA forces companies to address societal harms but is not too prescriptive on how they should do it. However, Allen also pointed out that there are holes in the text of the DSA. Part of the negotiations for the DSA were politicized, and as a result, there was a lack of ambition in topics such as the protection of personal data and recommender systems. Allen referred to what she sees as two significant challenges regarding DSA. The first is to prevent the DSA from becoming an empty tick-box exercise, especially regarding due diligence obligations. The second challenge is that DSA enforcement overwhelms the European Commission and national regulators and becomes weak, resulting in an inadequate protection of human rights. Allen made the case to ensure that civil society organizations are engaged in DSA enforcement. She also warned about the risk of regulatory capture in the auditing process to ensure that companies meet the obligations imposed by the DSA.

Mathilde Adjutor – Senior Policy Manager at CCIA Europe – first highlighted the openness of regulators in engaging with companies and praised the mostly timely preparation of secondary legislation. Next, Adjutor addressed the DSA shortcomings. The most obvious one is that some national regulators have not yet been appointed, even if the DSA is already fully applicable; this, she warned, impacts the law's implementation. Secondly, Adjutor talked about the fact that certain secondary acts, such as the methodology on counting the number of users or on data access for researchers, are still missing. There is also a lack of clarity on which other secondary acts are expected and the timeline for their adoption. In addition, some of the acts that are being approved, like the guidelines for election integrity, have been put forward quite late in the process, when companies have already been preparing for the European elections for months. Adjutor also shared her impression that much of the feedback received from stakeholders appears not to have been taken

into account by the European Commission. She also referred to the lack of a common definition of what a successful implementation of the DSA means – for some, it seems to be significant fines, while for others, sanctions would be a compliance failure. For the industry, successful implementation would be seeing DSA compliance built on the cooperation of all actors. Adjutor also highlighted the need for more staff in the European Commission and national regulators, a consistent application of the DSA across all EU member states, and more regulatory stability.

Joan Barata – Senior Legal Fellow at The Future of Free Speech – discussed the DSA's risks to freedom of expression. Barata pointed out that freedom of expression has not been central to the discussions regarding the DSA. The references to freedom of expression have been more declarative than substantive. The DSA provides little clarity on how companies should incorporate freedom of expression in their policies and practices, particularly when balancing this right with other interests like online safety. There are laws and court decisions in some countries like Poland and the United States that try to address how to conduct this balancing act, but it is still an open question, and the DSA does not solve it. Barata also referred to certain mechanisms in the DSA that may promote freedom of expression in platforms, such as transparency requirements and internal and external appeal mechanisms. However, Barata also warned that the entities that may be interested in getting accreditation to conduct external appeals will possibly be focused on online safety and be unlikely to prioritize freedom of expression. Barata also talked about the systemic risk assessments imposed by the DSA on very large online platforms and search engines. He warned that these assessments may result in companies being excessively restrictive of freedom of expression. Furthermore, the measures adopted to tackle these systemic risks may be adopted in private agreements between regulators and companies and not subject to public scrutiny. Barata also highlighted that the European Commission is a political institution that may be subject to political pressure when enforcing the DSA, which is particularly concerning given the law's impact on speech. He also warned that other countries outside the EU may misinterpret the DSA – willingly or unwillingly – and impose problematic restrictions on speech using the EU rules as a justification.

Panel 3: Governing Big Tech: The Role of the DSA and Other Digital Laws

The third panel was also moderated by Jordi Calvet-Bademunt – Research Fellow at The Future of Free Speech – and widened the lens on online platform governance, looking at market power and privacy, as well as online safety and freedom of expression.

Marco Giorello – Head of Unit at DG Connect, European Commission – discussed the European Commission's priorities regarding the DSA and the Digital Markets Act (DMA). The main priority is getting the entire supervisory structure in place – Giorello pointed out that the Commission has hired many staff members. Then, Giorello highlighted the work the European Commission has conducted over the last year, including the designation of the regulated entities for both laws and the opening of three formal investigations under the DSA against X, TikTok, and AliExpress. The investigations touch upon various subjects, such as tackling illegal content, protecting minors, and increasing the transparency and access to data by researchers. Regarding the DMA, Giorello reminded the audience that it became applicable very recently, but he stressed that the Commission would not hesitate to undertake investigations as it has done with the DSA. The last priority Giorello talked about was the launch of the joint work with national authorities; this is particularly relevant for the DSA, given that, along with the Commission, they are also in charge of enforcing the DSA. Regarding the relationship between DSA and DMA, Giorello said that the two laws present opportunities for synergy despite different approaches and objectives. These synergies will emerge as we go. The DMA is focused on fairness between big players and business users, while the DSA is broader and takes into account the balance between fundamental rights, societal risks, and other issues. Giorello explained that the DMA and the DSA are complementary because the two instruments originated from the same idea to increase the transparency and accountability of Big Tech companies.

Jan Penfrat – Senior Policy Advisor at EDRi – highlighted the opportunities that the DSA and the DMA present for Europe, in particular, to put guardrails in an industry that was allowed to behave in a way that would not have been accepted for other industries. The guardrails concern how companies moderate and manage our public spaces and use their market power. Penfrat warned that Big Tech companies have significant resources that enable them to weaken the DMA and the DSA and not comply with the law. He pointed out that the compliance measures proposed by some companies in the context of the DMA are clearly not in line with the purpose of the law, perhaps formally complying with its provisions but not really fostering competition in markets. Penfrat discussed the need for the European Commission to be aware of these tactics and be prepared to enforce the DMA and the DSA

effectively. He pointed out that, so far, he has been impressed with how the European Commission has been implementing these two laws.

Teodora Groza – Ph.D. candidate at Sciences Po Law School & Editor-in-Chief at the Stanford Computational Antitrust Journal – talked about the EU Data Strategy. Data is both a strategic competitive asset for digital companies and a key element of the fundamental right to privacy. Groza started by pointing out that prior to the adoption of the Data Strategy in 2020, in the EU data was only seen through the lens of privacy and fundamental rights. The Strategy changed that, promoting a discussion on the benefits of data flows and adopting a market-based rhetoric. Data was reframed as being the economy's lifeblood and a way to catch up with China and the United States. The narrative for the need for more data flows was based on the benefits competitive markets would bring for people. Groza pointed out that the EU Data Strategy is filled with language suggesting these benefits, like improved healthcare and other human-centric objectives. The Data Strategy is implemented through the Data Act – which empowers users to make use of the data that they generate in their smart devices – and the Data Governance Act – which creates a trusted framework for citizens to share and exchange their data. Groza also referred to the anti-Big Tech sentiment that seems to transpire from these laws, for instance, imposing strict requirements on the companies that may act as trusted data intermediation services.