FUTURE OF PRIVACY FORUM

Brussels Privacy Symposium 2022

Vulnerable People, Marginalization, and Data Protection

Symposium Report

Authors: Sebastião Barros Vale, Katerina Demetzou, Maria Badillo, and Christina Michelakaki

Editor: Isabella Perera

March 2023

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 US and around the world. FPF hopes to bridge the gap between European and US 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, workshops, Masterclasses, 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

On November 15, 2022, the Future of Privacy Forum (FPF) and the Brussels Privacy Hub (BPH) of Vrije Universiteit Brussel (VUB) jointly hosted the sixth edition of the Brussels Privacy Symposium on the topic of "Vulnerable People, Marginalization, and Data Protection." Participants explored the extent to which data protection and privacy lawincluding the EU's General Data Protection Regulation (GDPR) and other data protection laws like Brazil's General Data Protection Law (LGPD) safeguard and empower vulnerable and marginalized people. Participants also debated balancing the right to privacy with the need to process sensitive personal information to uncover and prevent bias and marginalization. Stakeholders discussed whether prohibiting the processing of personal data related to vulnerable people serves as a protection mechanism or, on the contrary, whether it potentially deepens bias.

The event also marked the launch of VULNERA, the International Observatory on Vulnerable People in Data Protection, coordinated by the Brussels Privacy Hub and the Future of Privacy Forum. The observatory aims to promote a mature debate on the multifaceted connotations surrounding the notions of human "vulnerability" and "marginalization" existing in the data protection and privacy domains.

The Symposium was started with short introductory remarks by **Jules Polonetsky**, FPF's CEO, and **Gianclaudio Malgieri**, Associate Professor at Leiden eLaw and BPH's Co-Director. Polonetsky stressed the importance of understanding that privacy increasingly intersects with other rights and issues. Malgieri offered an overview of VULNERA and incentivized participants to reflect on important questions, such as whether data protection law could serve as a means to address human vulnerabilities and marginalization.

Throughout the day, there were two keynote addresses by **Scott Skinner-Thompson**, Associate Professor at the University of Colorado Boulder and **Hera Hussain**, Founder and CEO of Chayn, a nonprofit providing online resources for survivors of gender-based violence, followed by three panel discussions, a brainstorming exercise with the Symposium's attendees in four different breakout sessions, and closing remarks delivered by FPF's Vice President for Global Privacy, **Gabriela Zanfir-Fortuna,** and the European Data Protection Supervisor (EDPS), **Wojciech Wiewiórowski**.

This Report outlines some of the most noteworthy points raised by the speakers during the day-long Symposium. It is divided into seven sections: the above general introductions; the ensuing section, which covers the remarks made during the Keynote Speeches; the next three that summarize the content of the discussions held during the panels; the sixth one that touches on the exchanges audience members had during the breakout sessions; and the seventh and final one that provides highlights of the EDPS's closing remarks.

2. Keynote Speeches: The Importance of Acknowledging Vulnerabilities and Inclusive Web Design

The first keynote speech of the Symposium, provided by **Prof. Skinner-Thompson, sought to outline the principles that should lead the ensuing discussion on data protection and vulnerability**. For Skinner-Thompson, it is essential to center and value the voices of vulnerable groups. He argued that the literature has explored vulnerabilities for many years without using the term "privacy" and that vulnerability and marginalization are dynamic and evolving conditions. He pointed out that privacy is not always considered a universal right under the law; for example, under US law, in order to maintain a right to privacy, individuals need to keep information completely private. According to Skinner-Thompson, this standard helps the privileged because they have the means to guard information privately and illustrates how neutral privacy frameworks may still, in practice, make certain groups vulnerable.

Skinner-Thompson added that privacy should not be an abstract right for marginalized populations since it is a key way to prevent substantial harm. Privacy can help vulnerable people in several settings, like protecting trans individuals from being subjected to violence and HIV patients from facing employment discrimination. The right to privacy also facilitates under-represented groups' speech and experiment while also helping them to choose and develop their identities and to increase their participation in the democratic sphere.

The other keynote speaker, **Hera Hussain,** explained Chayn's vision and approach to helping women and other groups subject to gender-based violence remain safe and thrive. Hussain stated that Chayn uses intentional web design to make the resources for survivors safer for all. In her presentation, the speaker explored Chayn's trauma-informed design principles, such as agency, accountability, and privacy, which can help test, rationalize, and question products, services, and strategic business decisions from a gender-aware perspective. She underlined that, due to stigma, victim blaming, and shame associated with gender-based violence, the need for victims' privacy is more significant.

In her presentation, Hussain provided a feminist perspective on data practices inspired by the work of Catherine D'Ignazio and Lauren Klein. She asserted that data is not neutral nor objective but rather a product of unequal social relations. This context is essential for conducting accurate, ethical analyses of online products and services. Furthermore, she stressed that some vulnerable groups could not foresee the risks that may arise from their data. Thus, data justice approaches need to be proactive in accounting for how people are counted, represented, and treated through the lens of data science.

3. The Role and Concept of Vulnerability and Marginalization Under Data Protection Law: Who is Vulnerable and How Should They Be Protected?

The first panel, "The role and concept of vulnerability and marginalization under data protection law: who is vulnerable and how should they be protected?," focused on identifying who is considered vulnerable, specifically in our data-driven society, and what means of protection should be put in place. It also touched on the tension between the need to provide enhanced protection for sensitive data and to rely on sensitive data to counter bias and discrimination. It featured **Malavika Raghavan**, Senior Fellow at FPF; **Kim Smouter**, Director General at the European Network Against Racism (ENAR); **Quirine Eijkman**, Deputy President at the National Human Rights Institute of the Netherlands, and **Joanna Szumanska**, Policy Officer at the European Commission, and was moderated by **Katerina Demetzou**, Policy Counsel for Global Privacy at FPF.

3.1 THE GDPR'S CLOSED LIST OF SPECIAL CATEGORIES OF DATA MAY NOT ACCOUNT FOR ALL VULNERABILITIES

Moderator Demetzou began the discussion by asking **Malavika Raghavan** whether intersectionality should constitute an important element of vulnerability and whether the data protection legal framework is well-equipped to protect vulnerable individuals. Raghavan made an initial point that vulnerability does not exist in a vacuum but, rather, within a structure that creates and reinforces it. The speaker drew lessons from lower-income communities in India and how financial inclusion through alternative data is fueling changes in India's social structure. Because such inclusion happens through mobile phones, which are not as widespread in rural areas, Raghavan observed that reliance on this technology is actually fueling marginalization. According to Raghavan, gender dynamics also play a role, as women in the Global South use but generally do not own mobile phones. Thus, organizations must understand whose data trail is being captured: the device owner or other device users.

Raghavan also questioned whether classifying and categorizing types of personal data as sensitive — including children's data — offers additional protection or whether it reproduces harmful effects. The speaker admits that classification and categorization are fundamental to human nature since they enable individuals to create a cognitive map of the world. However, Raghavan argued that the GDPR's 'list — based approach' to sensitive data and whether it effectively protects vulnerable individuals should be evaluated. The speaker argued that the list cannot aim to be universal but should instead be contextual depending on the particularities of each jurisdiction and how different data points come together. On this note, Raghavan highlighted that even if initial individual data points are non-sensitive, combining them can ultimately reveal sensitive personal data.

Raghavan also raised issues around the concept of the "average" or "reasonable data subject" and how they can exercise their rights. Asking whether a marginalized person can exercise their rights, she raised a hypothetical example of a woman from a non-privileged caste in India that has suffered some type of online violation. In this case, not only are the chances that this woman complains online extremely low, but also the user interface will likely not help, given that the design is not tailored to the particularities of highly marginalized groups. This situation illustrates

how design choices in the digital sphere influence decisions that can be and are made by individuals. According to Raghavan, web designers should be in the same room with legislators and regulators and should seek user feedback whenever possible.

3.2 VULNERABILITY LIES IN THE ESSENCE OF ALL HUMAN RIGHTS

Taking a broader perspective on fundamental rights, Demetzou asked **Quirine Eijkman** to explain the role of vulnerability within human rights discourse using her experience at the Dutch Human Rights Council. Eijkman began by saying that professionals tend to become so specialized that they usually see their field as the primary basis through which vulnerability surfaces. However, it is essential to consider the whole spectrum of human rights as a collective since vulnerability is what lies in the essence of the rights.

Eijkman referred to a scandal involving the Dutch government's monitoring of childcare allowances fraud as an example of how individuals can become vulnerable in relation to at least two human rights: the protection of personal data and access to justice. In this case, people were labeled by a risk classification system on whether they were likely to commit fraud. Where citizens had dual nationality, the assigned risk score would be higher. While that system seemed neutral, Eijkman asserted that, in reality, it was not. She was surprised that citizens had not filed any complaints on the matter to the Dutch Human Rights Council. Through this example, the speaker wished to highlight that vulnerability is not just about who is included but also about who is oppressed.

Eijkman mentioned that the Dutch Human Rights Council is also the Equality Body of the Netherlands. The speaker highlighted that most complaints are filed by people with disabilities and stressed the need to engage in meaningful dialogue before one reaches the stage of filing a complaint. In the Council's 2020–2023 Strategic Program, the chapter on Digitalisation and Human Rights focuses heavily on discrimination in the labor market, especially involving AI-driven recruitment and selection. Groups of individuals who are vulnerable in the labor market are usually already vulnerable and have difficulties in accessing the labor market in the first place, like women and ethnic minorities. Lastly, while Eijkman encouraged people to keep filing complaints, she noted that the focus should be on a long-term and preventive monitoring approach so as to achieve effective protection for vulnerable individuals and groups.

3.3 THE EUROPEAN COMMISSION'S APPROACH TO VULNERABILITY: NO HARMONIZED DEFINITION, BUT VARIOUS GROUNDS FOR ACTION

Demetzou asked **Joanna Szumanska** about the European Commission's approach to the concept of vulnerability and whether there is a standardized definition or are future plans to deal with the topic in a more targeted way. The question also concerned the Commission's recent guidance on enhancing equality data collection.

Szumanska first clarified that there is no harmonized definition of vulnerability at the EU level because vulnerability is a dynamic, context-based, and vague term. In her opinion, it is better to leave the definition of the term to member states. However, Szumanska also presented a tentative definition of vulnerability as "the state of being exposed to the possibility of being harmed physically,

emotionally, or otherwise because one belongs to a certain group." What is crucial, in her view, is to understand vulnerability in a particular context.

Szumanska also talked about the Commission's current approach to addressing vulnerability and discrimination and its future plans regarding these matters. In the field of non-discrimination, there are six grounds, equally important, on which vulnerability is assessed: sex, age, disability, racial and ethnic origin, religion or belief, and sexual orientation, all of which come from Articles 10 and 19 of the Treaty on the Functioning of the European Union. She clarified that those grounds are specifically regarding people who are vulnerable because they are at risk of discrimination. Article 21 of the European Charter of Fundamental Rights expands the list of grounds by adding factors such as political opinions and genetic factors.

However, according to Szumanska, vulnerability is much more than people being at risk of discrimination, as she enumerated some of the Commission's initiatives on vulnerable groups. First, she mentioned the "EU Justice Scoreboard," which is the annual cooperative information tool that aims to increase efficiency in Member States' justice systems. This tool takes into account the aforementioned six grounds, as well as the victims of gender-based violence and people seeking asylum. The Commission has additionally published the "Gender Equality Strategy 2020–2025," the "LGBTIQ Equality Strategy 2020–2025," the "EU Anti-Racism Action Plan 2020–2025," the "EU Roma Strategy Framework 2020–2030," the "Strategy for the rights of persons with disabilities 2021–2030," and the "EU Strategy on combating antisemitism and fostering Jewish life." Lastly, the speaker announced the Commission's plan to adopt a legislative proposal to strengthen the role of Equality Bodies.

Lastly, Szumanksa touched on the collection of equality data. She started by pointing to the European Handbook of Equality Data's definition of "equality data": "any piece of information that could be useful for the purpose of describing or analyzing the state of equality." This information could be qualitative or quantitative in nature and could include aggregated data that reflects inequality. According to Szumanska, comprehensive and reliable equality data is very useful for policymakers to assess the scale and nature of discrimination. The Commission encourages Member States to increase the collection of equality data. In February 2018, a subgroup on equality data was established as part of the "High-Level Group on Non-Discrimination, Equality, and Diversity." This subgroup functions as a platform to achieve an aligned approach and assist EU member states' equality data collection efforts. Lastly, Szumanska argued that the collection of equality data is allowed under the GDPR by mentioning the role of Article 9(2)(a) data subject consent.

3.4 THE ARTIFICIAL INTELLIGENCE ACT DOES NOT GIVE A VOICE TO MARGINALIZED GROUPS

Demetzou turned to **Kim Smouter** to discuss the vulnerability in the context of artificial intelligence. The moderator noted how the proposed EU AI Act (AIA) suggests criteria that could determine vulnerability: Articles 5 and 7 AIA refer to "vulnerable people" and make specific references to the criteria of "age, physical, or mental disability," as well as to "imbalance of power, knowledge, economic or social circumstances, or age." Demeztou asked Smouter whether the European Commission's proposed approach was comprehensive enough to tackle AI-driven biases and discrimination.

Smouter started by highlighting that the AI Act misses some points, primarily intersectionality. The AIA appears to choose specific characteristics while ignoring other ones, leaving open the question of who determines who is vulnerable in the context of the design and deployment of AI systems. People from vulnerable and marginalized communities do not have the power to influence such decisions. According to Smouter, this exclusion creates or enhances vulnerability in these environments and communities — as highlighted by the Dutch example Eijkman presented earlier. Smouter concluded by saying that having a list of criteria or vulnerable groups does not solve the problem because this approach misses the core of the issue: the historical and systemic nature of vulnerability. According to him, the proposed AIA does not take into account the ecosystem that creates vulnerability, which is necessary to solve the problem.

Then Demetzou asked Smouter whether he found any tension between the heightened protection afforded to sensitive personal data and the processing of this data for the purpose of building non-discriminatory AI systems, as proposed under Article 10(5) AIA. Smouter picked up Szumanska's last point on equality data collection and stressed that the GDPR does not prevent the collection of this information nor does it ban its processing. According to Smouter, the GDPR should not be used as a proxy to prevent the analysis of how much racism and discrimination there is in the EU; this data should actually enable researchers and policymakers to understand how large the problem is. In his view, the same reasoning applies to AI. Thus, there should not be limits to the collection of equality data, but instead, the proposed AIA should create safeguards that would apply whenever sensitive data is processed. Smouter argued that AI system designers should take into account that the processing of sensitive data can have a large impact on vulnerable groups, and therefore strong safeguards should be in place. Lastly, he stated that legislation could not solve all the problems related to marginalization because the legislation itself is part of the issue by not taking into consideration the voice and lived experience of vulnerable individuals during the lawmaking process.

4. Assessing Data Processing Impacts on Vulnerable and Marginalized Populations: What Is The Role of Harms, and Can We Measure Them Without Processing Sensitive Information?

The second panel, "Assessing data processing impacts on vulnerable and marginalized populations: what is the role of harms, and can we measure them without processing sensitive information?," focused on identifying the term "harm" and assessed whether Data Protection Impact Assessments (DPIA) as formulated under the GDPR could effectively account for data subjects' or affected individuals' vulnerabilities. It featured **Helena Koning**, Europe Data Protection Officer (DPO) at Mastercard, **Tanya Krupiy**, Lecturer in Digital Law, Policy, and Society at Newcastle Law School, **Sarah Chander**, Senior Policy Adviser at European Digital Rights (EDRi), and **Dale Sunderland**, Deputy Commissioner at the Irish Data Protection Commission, and was moderated by **Prof. Gianclaudio Malgieri**.

The speakers touched on the impact of data technologies on vulnerable and marginalized groups. The notion of "harm" to fundamental rights presents problems in legal terms, in its ambiguous position between damages and less significant effects. Data Protection Impact Assessments (DPIAs) may be useful tools, but there is still little guidance on how particular forms of vulnerabilities might be addressed and mitigated. The panelists discussed the existence and adequacy of current regulatory tools and frameworks and how they could be improved to take vulnerabilities into account.

4.1 THE IMPORTANCE OF QUALIFYING AND QUANTIFYING HARM

Moderator Malgieri first turned to panelist Tanya Krupiy to question whether it is possible to quantify harm and, if so, how it surfaces in data processing contexts. Krupiy indicated that first, one must define "harm" and how to locate it. It is important to think outside of the box to find solutions because the current paradigm is limiting. She argued that using proxies to quantify harm could be helpful but that one must keep in mind the qualitative component of harm. Secondly, Krupiy highlighted the need to move beyond assessing the harm to the individual to the harm at the collective level, notably with the assistance of AI-derived insights.

Moreover, Krupiy opined that thinking about scales between individuals or the collective is the wrong approach because both are interconnected. However, according to her, it should be acknowledged that countries have embraced collecting more data on populations, which could make perverse incentives emerge even while giving off the image that states are becoming technologically savvy.

Finally, Krupiy stressed that focusing only on the GDPR may miss the structural dimensions of inequality. She argued for the necessity of reframing and specifying how the GDPR can help understand or engage with structural inequality.

4.2 THE ROLE OF SUPERVISORY AUTHORITIES AND ACCOUNTABILITY TOOLS WHEN ASSESSING RISKS

Malgieri then turned to Dale Sunderland about the role that Data Protection Authorities (DPAs) can play with *ex ante* guidelines and strategic enforcement actions. On this note, Sunderland began by recalling that the GDPR is fundamentally a risk- and principles-based law. However, he added

that risks should be calculated according to the context and circumstances. Sunderland mentioned that, at the Irish DPC, they give careful consideration to what "risk to the rights and freedoms of a natural person" is in a particular case, especially regarding potential harm to persons in a vulnerable position both as groups and as individuals. He added that the DPC's assessment is always context-based and as objective as possible, depending on the nature of the processing of personal data and who it targets, which organizations should also consider when planning data processing activities.

In this context, Sunderland indicated that DPIAs might be useful tools, while controllers should consider the broader context of the GDPR. An example is how Article 25 on data protection by design and by default requires data controllers to implement appropriate technical and organizational measures both when determining the means of processing and at the time of the processing itself. Sunderland stressed that DPIAs fit within this structure but that organizations can only effectively identify the cohorts of individuals who will be affected by the processing if they hear from them and understand their perspectives.

Finally, Sunderland outlined the ability of DPAs' extensive regulatory toolboxes to enable the consideration of vulnerabilities within the context of personal data processing. According to Sunderland, the toolbox includes measures like:

- **Issuing additional guidance:** Despite the fact that DPAs are somewhat limited in defining what "harm" is and that "taxonomies of harm" would not be enough to provide a satisfactory definition, Sunderland argued that DPAs can focus their effort on understanding what "risks" are and mapping harms that may flow from those risks.
- **Following up on evolving interpretations:** For example, Sunderland pointed to an August 2022 ruling where the Court of Justice of the EU (CJEU) broadened the scope of Article 9(1) GDPR on special categories of data. On the upside, the ruling shows that the CJEU is looking at more pieces of data as sensitive, thereby affording them more protection. On the downside, some theoretically less risky processing activities may now fall within the Article 9 GDPR prohibition. Thus, companies must review whether they are dealing with sensitive data in a broader sense and be ready to comply with the law. Lawmakers must also think more deeply on how to allow the processing of special categories of data for benevolent purposes — with adequate safeguards and due regard for proportionality — without the need for explicit consent.
- **Enforcing existing regulation and guidance:** For example, Sunderland pointed to the Irish DPC's guidance on children's data protection, an area where the quantification of risk and impacts matters. According to the DPC, online services directed at or intended to be accessed by children have a higher bar in terms of complying with the GDPR because of objectively higher risks and children's special status.

4.3. A NEED FOR TRAINING AND INVOLVING DATA PROTECTION OFFICERS AND PRIVACY EXPERTS

In reaction to Sunderland's remarks, Malgieri highlighted the existing connection between risks and groups of vulnerable people. He argued that before looking at risks or harms, controllers could look at who the affected people are, or, the other way around, to know who is affected by the processing, controllers could assess the type of risks or harms first. On this note, he asked **Helena Koning** about

her experience as a DPO accounting for vulnerable people in daily compliance, the performance of DPIAs, and the implementation of privacy by design.

Koning started by highlighting that DPOs must keep learning throughout their careers and continuously build bridges with their appointing entities. Koning stressed that Mastercard's privacy teams and DPO's office significantly focus on these populations and research how they are potentially impacted. According to her, companies should prioritize inclusion that does not impact customers' privacy. An example is how Mastercard implemented accessible design to bring security, inclusivity, and independence to blind and partially sighted cardholders in their new debit and credit cards, which now have a round, triangle, or squared indent for visually-impaired people to actually "feel" the cards so that they can identify them.

Koning also mentioned Mastercard's digital identity program for refugees. Even though digital identity can be complex from a privacy perspective because of the use of sensitive data like biometrics, there could be significant benefits for the more than 1 billion people worldwide who lack trusted identifying credentials or birth certificates. For Koning, it is as important to consider the potential benefits for data subjects as the potential privacy risks when evaluating products. This exercise starts with understanding the population for which the product is designed and how it will be used.

Moreover, Koning indicated that privacy is largely about guidance, training, and awareness for the staff designing digital solutions. From Koning's perspective as a DPO, these individuals should learn to ask whether additional safeguards are needed or to reframe the focus: "should we do something more or do something less to address the issue?" According to her, this is particularly important when dealing with data protection principles, such as data minimization in the context of age verification technologies or the processing of sensitive data to provide additional benefits. In those cases, Koning argues it is essential to reinforce other controls, such as providing more encryption, access management controls, and transparency.

4.4. THE NEW EU PROPOSALS AND THEIR IMPACT ON DATA PROTECTION FOR VULNERABLE PEOPLE

Malgieri then turned to **Sarah Chander** to ask whether the new EU legislative proposals from the European Strategy for Data would adequately address issues related to technology-enabled marginalization. Chander began by indicating that most of EDRi's advocacy work consists of using the principles of the GDPR to pose broader questions concerning the new legislative proposals at the EU level. They adopt this approach since the inherent basis of the GDPR is the protection of fundamental rights in the face of data processing, which should remain the point of focus in digital policymaking discussions.

However, Chander claimed that the new proposals and their relation with fundamental rights have a different approach than the GDPR. She argued that these proposals assume that more digitalization and data processing is necessary and beneficial for society, which is not the case. As an example, the AI Act, as an EU internal market regulation, starts with the assumption that AI systems are inherently good, and thus the use of AI should be facilitated. Like other proposals, the text assumes that all persons are affected by digitalization in the same ways without considering the possibility of a variety of experiences and potential harms to different groups.

Chander then dived deeper into her concerns around the AI Act. First, she warned against processing sensitive data to prevent bias or discrimination, as proposed under Article 10(5) of the Proposal, as it appears contradictory to the GDPR's principle of data minimization. While Article 10(5) is, in theory, a "good approach" that has received support from academics, it should not be seen as the only approach for addressing discrimination generated through AI systems. Second, Chander argued that policymakers and regulators should distinguish between AI systems that are "good" because they were inherently designed for good and cannot be repurposed (i.e., a 1:1 facial recognition system for verification when accessing a service) and AI systems that are used for automated decision-making, predictive policing, or other areas that determine crucial aspects of individuals' lives, such as whether or not they get a job. According to Chander, AI systems that inherently discriminate against certain vulnerable groups should be forbidden. Third, she stated that individuals need access to more tools and broader justice frameworks that allow them to challenge decisions made by AI systems, even beyond their GDPR-assigned rights, which are currently absent from the draft AI Act.

According to Chander, beyond the European Data Strategy, some legislation proposed at the EU level in the space of migration and law enforcement seems inherently contradictory to the principles of the GDPR, including data minimization and purpose limitation. One of those cases is the Proposal for a Regulation on Asylum and Migration Management, which proposes to collect child migrants' biometric data. Another is the European Commission's Proposal to criminalize gender-based violence online, which addresses the issue of vulnerability and marginalization but does not properly account for how women and other persons are affected by such violence and creates a risk of exposing or censoring them. For Chander, these cases illustrate that individuals have different *de facto* and *de jure* access to privacy and data protection.

Similarly, Koning, during her intervention, also focused on other proposed or recently approved EU laws that touch on data protection, as well as the challenges in these contexts. She discussed the interplay between the GDPR's rules on age verification, which are limited to information society services, and specific age-appropriate requirements under the Digital Services Act (DSA). This new law also mandates systemic risk assessments for large online players, which should consider children and vulnerable groups, in addition to mandatory DPIAs under GDPR. For Koning, the introduction of new requirements in this space makes compliance more difficult and presents a need for clearer and more consistent guidance, templates, and standards.

However, Koning also highlighted the opportunities offered by new pieces of law to empower individuals and vulnerable groups. Under the Data Governance Act (DGA), there are rules regarding data altruism and data cooperatives, which would give people an opportunity to donate data to find new insights about and offer benefits to persons with vulnerabilities. Koning is optimistic about the positive impact that these types of initiatives could have on the LGBTQI+ community and victims of gender-based violence.

5. Protecting Preventively and Proactively: Promoting Participation, Mitigating Risks, and Adjusting Design

The third and final panel, "Protecting preventively and proactively: promoting participation, mitigating risks, and adjusting design," focused on whether and how proactive approaches in the GDPR and other data protection laws like Brazil's LGPD can guarantee more effective protection for vulnerable people. It featured **Alessandra Calvi**, Ph.D. Candidate at the VUB's Law, Science, Technology & Society (LSTS) Group, **Rafael Zanatta**, Executive Director at the Data Privacy Brasil Research (DPBR) Association, **Adam Bargroff**, Public and Privacy Policy Manager at Meta's Trust, Transparency, and Control (TTC) Labs, **Grace Mutung'u**, Project Lead at the Open Society Foundation (East Africa), and was moderated by **Sebastião Barros Vale**, EU Policy Counsel at FPF.

5.1 THE EFFECTIVENESS OF DPIAS IN PROTECTING VULNERABLE POPULATIONS

Alessandra Calvi started the conversation by explaining that GDPR tools like DPIAs could be effective methods to protect vulnerable and marginalized groups but that they are not sufficient. For Calvi, DPIAs present certain advantages. First, the data controller can take appropriate technical and organizational measures to protect vulnerable people depending on whether their rights are at risk; this approach can help to better assess which people require protection since the closed list of Article 9 GDPR may not always help to this end. Second, DPIAs as *ex ante* tools prevent damages and harms and the need to adopt *ex-post* remedies.

However, Calvi also identified some shortcomings of DPIAs. She underlined that DPIAs do not challenge the power dynamics of processing since data subjects will only be involved in the assessment, and thus their opinions accounted for, when the data controller deems it appropriate. Furthermore, Calvi noted that there are no transparency obligations vis-à-vis data subjects concerning DPIAs. Therefore, for DPIAs to protect individuals and vulnerable groups, Calvi suggested that the GDPR should introduce such transparency duties and grant individuals a right to force controllers to conduct a DPIA.

Calvi also touched on "smart cities" and their relationship with the GDPR. In her view, smart cities are complex ecosystems with many actors (both private and public) that interact with each other and process citizens' personal data. In this context, data subjects are particularly vulnerable, as the application of certain GDPR safeguards is not always straightforward. For example, it is not always clear which data should be considered as personal nor how citizens should be informed of the processing of their personal data. Finally, Calvi mentioned that certain data subjects are democratically underrepresented and thus not able to affect decision-making in smart cities. In the latter context, she argued that GDPR might need to be complemented by other tools for tackling biases, such as the AI Act.

5.2 WEB DESIGN SOLUTIONS FOR THE PROTECTION OF VULNERABLE POPULATIONS

Adam Bargroff offered an industry perspective on the role that online interface design can have in ensuring the protection of vulnerable people in the digital space. Bargroff started by explaining what TTC Labs is and how it operates; as an industry initiative supported by Meta, it focuses on

better privacy-centered user experiences, including those around notice and consent, as well as explainability and user control in AI-driven services. He stated that TTC Labs brings experts — like academics, designers, policymakers, and civil society representatives — into the room to collaborate on possible design solutions and share the outcomes.

Bargroff argued that interactive focus groups can play an important role in understanding people's needs. Such an approach, in combination with TTC Labs' best interests of the child framework, helped TTC Labs to develop a code design program on autonomy and parental supervision for child-focused services.

He then touched on whether AI explainability requires adjusting explanations to each user for them to adequately understand AI systems. Bargroff talked about two projects that TTC Labs has led on this matter; the first relied on external experts' inputs on AI transparency, control, and data use in online services; the second was based on workshops where they gathered user experiences around data use to understand their transparency needs. For Bargoff, these types of projects facilitate the adoption of strategies that map well to GDPR requirements and increase transparency for data subjects, especially for marginalized ones. According to him, this can be achieved via step-by-step transparency mechanisms that are complemented by visual aids, as well as through personalized transparency approaches that enable people to interrogate how they experience the services they are using. In reaction, **Barros Vale** added that the users of online services have different expectations about the amount of personal data used by services and the extent of their personalization. This was also reflected in a September 2022 Opinion by the CJEU's Advocate General Rantos, which emphasized that it is important to ensure each person has a level of transparency that is adjusted to the nature and complexity of the digital service at hand.

5.3 VULNERABLE GROUPS IN AFRICA: THE CASE OF KENYA'S DIGITAL ID SYSTEM

Grace Mutung'u touched upon the Kenyan proposed digital ID system, which she litigated against. She explained that the idea was to transform an existing national ID system into a digital system via biometrics. The contestation in Kenya focused on three aspects:

- There was not enough transparency and public participation regarding the ongoing changes;
- Kenya did not have a data protection regime in place, and thus the project challenged privacy and data protection; and
- The project generated discrimination, as it excluded individuals from isolated places or who had no prior documented proof of identity.

Mutung'u also underlined that the power governments could obtain from digitalization, especially when it is mandatory for citizens, is significant. Therefore, it is crucial to first decide who will be in charge of the data, who will have access to it, and what happens if a citizen has issues or wants to raise grievances. She added that in the context of digital IDs, it is advisable to consider the needs of the most vulnerable and the concept of "collective privacy," as there has not been enough reflection on collective rights as a means to protect vulnerable people and the risk of facing discrimination. She pointed to environmental law for inspiration and a better understanding of plural identities.

Finally, Mutung'u touched upon the role of discussions about vulnerability and marginalization in enacting data laws in Africa, as well as whether such laws are seen as instruments for the empowerment of vulnerable groups. She argued that data protection laws could be the "solution" to the issues brought about by digitalization. In the Kenyan example, a data protection law was a precondition for the digital ID project to move forward. Since that controversy, there has been a new litigation "trend" in Kenya towards demanding the national government to conduct a DPIA of the digital ID project. For Mutung'u, once more African countries have data protection laws in place, vulnerable groups will be better protected, and African jurisdictions will be eased. However, she also argued that it is important not to think of privacy and data protection as existing in a vacuum but rather in the context of safeguarding other rights and non-discrimination; this is an approach that civil society organizations are currently pursuing.

5.4 NAVIGATING DATA PROTECTION AND SOCIAL JUSTICE IN BRAZIL: CHALLENGES AND STRATEGIES

The last speaker of the panel, **Rafael Zanatta**, stressed that Brazil is a deeply unequal society with structural racism and serious problems of police violence towards minorities. He explained that his NGO — Data Privacy Brasil Research (DPBR) — takes into account two key elements in its campaigning efforts; social justice and asymmetries of power. More specifically, in 2020, they set up a partnership with public defenders from Rio de Janeiro and São Paulo. Zanatta underlined that public defenders are the most appropriate individuals to involve when working with local communities, given their constitutional mandate to protect the poor and vulnerable.

In their engagement with local communities, DPBR had to first understand how people felt about data protection; DPBR could not simply ask individuals for their general views but instead had to pose the right questions on specific issues such as facial recognition, child protection, and police surveillance. DPBR's surveys showed that people were primarily concerned about the processing of data by private actors and the risks children may face using online services like TikTok. For Zanatta, it is crucial to approach communities' concerns by first looking at their lives and only then moving to the theoretical discourse of their digital rights.

Then, he touched upon Brazil's General Data Protection Law (LGPD), its potential to address social injustices, and its similarities to the GDPR. He noted that even though the legislation explicitly tackles inequalities by adopting a principle of non-discrimination, the provisions related to DPIAs are weaker. This weakness stems from the fact that it is not mandatory to conduct a DPIA, and the legislation does not provide differentiations on whether there is a high or low risk for data subjects. Thus, Zanatta explained that the Brazilian DPA (ANPD) is currently trying to elaborate on what constitutes a high risk and should trigger controllers' obligation to carry out a DPIA.

Lastly, Zanatta mentioned that since Brazil has a very strong system of class actions and collective rights, civil society is currently focusing on demanding certain rights through litigation. As an example, he pointed to a 2019 case concerning the São Paulo metro that had set up an AI system with cameras for the purpose of predictive policing, which affected 14 million people. Along with other organizations and public defenders, DPBR filed a complaint against the system, asking to see the DPIA and an explanation of the reasons behind the installation of the cameras. The legal

argument was based on LGPD Articles 18 (data access right), 6 (principle of non-discrimination), and 2 (information of self-determination) and led to the Supreme Federal Court of Brazil's creation of the concept of collective self-determination, which consisted of positive obligations to involve with communities and ensure public participation when designing these types of systems.

6. Have Your Say: What Is Vulnerability, Why, and How to Address It?

Next, the Symposium broke out into four sessions to engage and receive feedback from the participants. Led by an individual convener, each breakout group focused on a different topic related to the overall proceedings of the Symposium and attempted to gather the opinions of audience members on a range of issues pertinent to the intersection of vulnerable and marginalized groups, data protection, and technology. After the sessions, the conveners presented a summary of the discussions.

Muhammed Demircan, BPH's Managing Director, led a group on "Vulnerable consumers and data power: lessons from the DSA and DMA." **Katerina Demetzou**, FPF's Policy Counsel for Global Privacy, conducted a session focused on what it means to be vulnerable and explored power imbalances online and offline. **Vincenzo Tiani**, BPH's Programme and Dissemination Coordinator, convened a group that explored "Vulnerability in the context of AI: ensuring fairness and mitigating biases." Finally, **Hunter Dorwart**, a Policy Counsel at FPF, led a discussion on the role, successes, and shortcomings of applying existing data protection law to mitigate vulnerabilities and its effects.

7. Closing Remarks by Dr. Wojciech Wiewiórowski, *European Data Protection Supervisor*

To wrap up the Symposium, FPF's Vice President for Global Privacy, Gabriela Zanfir-Fortuna, had the honor to thank all the participants and attendees for their contribution to the debate and to introduce the EDPS, Dr. Wojciech Wiewiórowski, for his closing remarks.

In his intervention, the EDPS acknowledged the fragility of the human condition and that the **discussions around vulnerability in data protection circles have unfortunately been scarce**. According to the EDPS, this perspective should be at the core of reflections on potentially harmful data processing practices. Furthermore, Wiewiórowski pointed to the various ways in which people are marginalized: through language, populism, fears, and prejudices at the EU's borders, where increasing data collection is used to keep asylum seekers away; by denying equal rights to data subjects across the EU, who often see their complaints dropped without justification or abusive data practices not monitored closely enough by DPAs; through the blind belief in exclusively beneficial outcomes of new technologies, of which children are some of the most noteworthy victims.

To conclude, the EDPS encouraged the Symposium's participants to continue to speak up against data-fueled injustices and expressed his hope that the debates during the event could give a representative voice to those currently suffering in silence.

To learn more about FPF in Europe, please visit fpf.org/about/eu.

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

fpf.org