Reimagining the Data Subject in GDPR

Introduction

Scholarship centering marginalized groups has long questioned the universality of a "default" person. In her landmark text *Justice, Gender, and the Family*, feminist philosopher Susan Moller Okin argues that "almost all current theories continue to assume that the 'individual' who is the basic subject of their theories is the male head of a fairly traditional household."[1] Professor Donna Haraway's framework of the "view from nowhere" shows that a supposedly universal perspective, which she calls the "God trick," can actually shield a "very specific position (male, white, heterosexual, human)."[2] In the words of bestselling author Caroline Criado Perez, "this reality is inescapable for anyone whose identity does not go without saying, for anyone whose needs and perspective are routinely forgotten. For anyone who is used to jarring up against a world that has not been designed around them and their needs."[3] Political philosopher Iris Marion Young writes that "[t]he privileged groups lose their particularity; in assuming the position of the scientific subject they become disembodied, transcending particularity and materiality, agents of a universal view from nowhere. The oppressed groups, on the other hand, are locked in their objectified bodies, blind, dumb, and passive."[4] Without explicitly mentioning race, gender, or any other aspect of identity, an abstract conception of subjecthood runs the risk of insidiously adopting the identity at the top of the societal hierarchy. When a certain level of abstraction is necessary, is there a way to universalize more inclusively, to affirmatively elevate the worldviews of those traditionally left out of the narrative?

Susan Moller Okin criticizes theorists of justice for "tak[ing] mature, independent human beings as the subjects of their theories without any mention of how they got to be that way." Quoting Hobbes, she notes that theorists of justice neglect the moral development of their subjects, as though they just sprung out of the earth like mushrooms. This neglect has the fundamentally gendered implication of erasing predominantly female unpaid labor in childcare and moral education.[5] It also erases historical oppression and inequalities among subjects, starting from the illusory premise of mature individuals who emerged on a level playing field. Building theories of justice on the interactions between the individual subjects of state-of-nature thought experiments without developing a more inclusive vision of the subjects themselves hinders the pursuit of justice. Similarly, law professor Shreya Atrey asks: "[H]ow does the complexity of difference come to be reflected in universality once we accept it as the premise of human rights?" Rather than abstracting away difference to create an ahistorical human rights subject, can we align with Hannah Arendt's vision of difference as universality? Understanding universality as intersectionality can change the basis for which rights are realized or violated and can shift the focus of law to transforming social structures.[6]

In 2018, the General Data Protection Regulation (GDPR), a landmark law at the forefront of data protection, defined a "data subject" as "an identified or identifiable natural person,"[7] a

[1] Susan Moller Okin, *Justice, Gender, and the Family* (New York: Basic Books, Inc., Publishers, 1989) 9.
[2] Donna Haraway, "Situated Knowledges: The Science Question," *Feminist Studies* (1988); Monika Rogowska-Stangret, "Situated Knowledges," *New Materialism* (2018).
[3] Caroline Criado Perez, *Invisible Women* (New York: Vintage Books, 2019).
[4] Iris Marion Young, *Justice and the Politics of Difference* (Princeton University Press, 2011).
[5] Okin, 9, 19, 21-22.
[6] Shreya Atrey, "The Humans of Human Rights," *Intersectionality and Human Rights Law* (2020).
[7] "Art. 4 GDPR: Definitions," *Intersoft Consulting*.

default person "ostensibly 'unmarked' by notions such as gender, race, and class."[8] Applying the reasoning outlined by Okin, Atrey, and other scholars, I posit that data subjecthood masks power dynamics under a veneer of universalism. How can we reimagine the data subject to advance data justice? Viewing the data subject as an entity *with data to provide* and *with rights over that data*, I draw from Aisha P. L. Kadiri's idea of the "paradox" of data protection–that we need protection both *through* and *of* data in order to reimagine a more inclusive data subject.[9] In Section 1, I explore Kadiri's conception of a bottom-up construction of the data subject–empowering communities to construct their own digital identities and take control of the narrative created by raw data. Raw data itself is rooted in history–we need to ask ourselves "which information needs to become data before it can be trusted, and whose experiences need to become data before they can be considered as 'fact' and acted upon." In Section 2, I build on Joana Varon and Paz Peña's analysis of Digital Welfare States[10] to demonstrate that assuming the data subject is pre-constituted prevents us from engaging meaningfully with the power structures in which that subject developed, thereby enabling data protection regulations to reinforce those structures.[11] In Section 3, I discuss a layered-vulnerability approach to reforming data protection, proposed by Gianclaudio Malgieri and Jedrzej Niklas,[12] in order to account for power asymmetries and to aspire towards universality as intersectionality.

1. The Data Approach

In this section, I describe Aisha Kadiri's work on an emancipatory, community-centered, and participatory framework for constructing a more inclusive data subject. The communities represented by this data subject have always existed and continue to exist, but they have been excluded from the digital portrait. This data approach protects historically excluded populations *through* data in order to promote data-driven policymaking to advance justice.

1.1. The AfroZensus

"Every time we go to politicians as a community, or as the communities and we ask for something, we make demands, they tell us, 'Yeah, OK, but where's the data to back this up?' And we're like, 'Yeah, OK, we don't have data, but also at the same time, you're refusing to gather that data.'" - AfroZensus co-leader Teresa Ellis Bremberger

Due to an ugly history of Nazism, in which population registers helped organize and streamline the Holocaust, Germany does not collect racial data of its citizens. This policy came under scrutiny during the 2020 BLM protests, as activists argued that a lack of data about people of color and their experiences of discrimination in Germany prevented serious institutional reform to advance racial justice. As Daniel Gyamerah, the chair of Berlin-based community empowerment project Each One Teach One, explained, "When it comes to statistics shedding light on racism, Germany is stuck in the stone ages. We simply don't have the data. And that makes it easy for those here who argue that institutional racism is a problem unique to the U.S. or the UK." Germany only collects data on citizens' "migrant background," which excludes people of color whose parents were born in Germany but nevertheless continue to experience racism; it also combines very different groups of people into one political community, glossing

[8] Jens T. Theilen, et al., "Feminist data protection," *Internet Policy Review* (2021), 10.
[9] Aisha P.L. Kadiri. "Data and Afrofuturism," *Internet Policy Review* (2021), 15.
[10] Joana Varon and Paz Peña, "Artificial intelligence and consent," Internet Policy Review (2021).
[11] Theilen, 14, 10.
[12] Gianclaudio Malgieri and Jedrzej Niklas, "Vulnerable Data Subjects," Computer Law & Security Review (2020).

over important nuances.[13] Moreover, equating migration with Blackness problematically conflates being nonwhite with being foreign.[14] Additionally, the German Federal Anti-Discrimination Agency only records self-reported discrimination cases; however, since Germany's equality body does not have the right to bring these cases to court or use them to influence policy, the incentive to self-report is low. Thus, German MP Karamba Diaby called for collecting anti-discrimination data.[15]

The AfroZensus–a federally funded survey project led by Each One Teach One and inspired by the U.S. Black Census Project as well as the Being Black in Europe survey–represents "[o]ne attempt to fill the gaping holes in Germany's statistical self-portrait."[16] The survey aims to identify policy issues and resources relevant to Black German communities, as well as collect data to bolster legislative lobbying and political organizing.[17] Importantly, this data collection effort was designed to be a participatory community-centered process, rather than a process of data extractivism targeting marginalized groups. For example, the AfroZensus empowers participants to choose their own identity terminology (such as "Black," "Afro-German," etc.) and centers their experiences of intersectional discrimination.[18] For the first time, Germany had empirical data on exoticization (90% of respondents reported having their hair touched without their permission), sexualization (nearly 80% of respondents reported having received sexualized comments on dating apps regarding their race), criminality (over 50% of respondents have been asked if they sell drugs and have been stopped by police for no apparent reason), and obstacles to confronting discrimination (more than 90% of respondents reported that people do not believe them when they describe their experiences with racism, and 75% of those discriminated against said they do not report cases of racism).[19] These statistics have always existed, but for the first time they gained visibility in Germany's statistical portrait.

Germany claims that it is race-blind, perpetuating the ideology that avoiding categories prevents the "creation" of racism ("Everyone is German").[20] However, the data gap resulting from this blind universalism "speaks volumes. . . . [I]f 'you're not counted, then you don't count.'"[21] Rather than "creating" racism, explicitly counting those excluded from the country's digital portrait provides marginalized communities with "the visibility as a group that is necessary for better advocacy."[22] However, the AfroZensus must address the concerns motivating the country's race-blindness: namely, the misuse of race-related data for surveillance and oppression. As AfroZensus co-leader Teresa Ellis Bremberger notes, "You can't just say, 'Oh, we're making a survey on Black people' because most people will be like, 'Why?' and 'Who am I sharing my data with?' and 'Is my data safe with you?' and 'Who is analyzing this?'"[23] Rather than refuse to collect data altogether, policymakers should adopt more safeguards around how data is gathered and used. For example, the AfroZensus, while funded by the government, keeps data on its own encrypted servers to protect the privacy of participants. Additionally, while the

[13] Aamna Mohdin, "Statistically speaking," *Quartz* (2017).
[14] Ekene Okobi, "The AfroZensus is an effort," *The World* (2021).
[15] Philip Oltermann, "France and Germany," *The Guardian* (2020).
[16] Oltermann.
[17] Okobi.
[18] Kadiri.
[19] "'Afrocensus' results," *dw.*
[20] Mohdin.
[21] Mohdin.
[22] "'Afrocensus' results"; "Afrozensus."
[23] Okobi.

project organizers worry that national conversations about race may lead to backlash from a xenophobic right-wing faction of German society, they believe in the power of recording "the realities of life, experiences of discrimination and perspectives of black, African, Afrodiasporic people in Germany" to further racial justice.[24]

1.2. An Afrofuturist Data Subject

"Rewriting the data subject thus entails the recognition of who has been an object for far too long in order to break down underlying exclusionary notions of who counts as human and therefore enjoys protection within that category."[25]

The AfroZensus provides an example of creating a data subject from the bottom-up, of protecting *through* data. By "making visible what is often deemed invisible," and "creating vocabulary for the Black experience in Germany," the AfroZensus "actively opposes the denying of Black people's existence in Germany as well as the denial of structural racism within the country." In "Data and Afrofuturism: An Emancipated Subject?" Aisha P. L. Kadiri argues that the data subject created by the AfroZensus accords with Afrofuturist theory, which offers a powerful lens for the emancipation of the data subject. Afrofuturism nurtures a "liberated and intersectional data subject" that "accounts for interconnectedness, unsettles predefined categories, and acknowledges the structural aspect of discrimination."[26]

The Afrofuturist data subject is radically subjective, collective, and contextual. *Radical subjectivity* transforms those historically objectified into the subjects and questions exclusionary assumptions about who counts as human and deserves data protection. For centuries black people have been relegated to objects of history rather than the subjects–in the words of Toni Morrison, "spoken of and written about" rather than in control of their own narrative. By gathering data on Black Germans as a group, using the participants' self-chosen terminology, and providing them with a platform to share their experiences of discrimination, the AfroZensus treats census respondents as the rightful subjects of their data story. *Collectivity* includes collective trauma, community-building, collective healing, collective memory, and identity formation, which are central to Afrofuturist storytelling. "Afrofuturism forms, reclaims, and enacts identity as a collective rather than individual and with no claim of universality," and the AfroZensus similarly helps construct a collective Black German data subject by aggregating experiences of discrimination to serve collective racial justice goals. The AfroZensus strives to answer the community-focused questions of "Who are we, what do we encounter, and what do we want?" Lastly, *contextuality* refers to an acknowledgment of social contexts and power dynamics in guiding data decisions. The AfroZensus creates the data subject in order to protect marginalized groups from power asymmetries and thus provides an inherently contextual alternative to a race-blind, individualistic, supposedly universal data subject that may not actually represent the interests of the most vulnerable members of society.[27]

An estimated 1.1 billion people globally have no formal government identity.[28] 81% live in Sub-Saharan Africa and South Asia, and 63% live in lower-middle income economies.[29] Technology can help provide digital identities that facilitate access to healthcare, education, and financial inclusion for the most vulnerable populations. "There is no time to waste, though we

[24] Okobi; "Afrozensus."

[25] Kadiri.

[26] Kadiri.

[27] Kadiri.

[28] "Identity in a Digital World," *World Economic Forum* (2018).

[29] Vyjayanti T. Desai, et al. "The global identification challenge," *World Bank Blogs* (2018).

must also remember that a poorly designed digital identity can be worse than no identity at all"; as digital exclusion tends to run along existing lines of oppression,[30] "[w]e need to safeguard against the possibility of making the lives of the most vulnerable people on the planet even more vulnerable."[31] I argue that an inclusively-designed digital identity involves reimagining the data subject. Digital identification, while necessarily individual in nature, can fit within a larger scheme of collective protection *through* data that helps advance collective aims such as racial and gender justice in the digital world. Perhaps the Afrofuturist normative framework and AfroZensus case study can provide guidance on establishing community-centered, participatory data collection programs that empower participants to own their data narrative and that thereby create radically subjective, collective, and contextual data subjects.

2. The Rights Approach

In Section 1, I discuss reimagining the creation of the data subject by acknowledging that raw data is a function of power structures. In Section 2, drawing from Joana Varon and Paz Peña's analysis of Digital Welfare States, I describe the dangers of assuming that the data subject is an apolitical individual always capable of making a free, meaningful choice despite an imbalanced playing field.

2.1. The Digital Welfare State

Recent years have seen a global rise in Digital Welfare States to automate welfare provision to citizens. In Colombia, a program called SISBÉN collects socioeconomic data from the population and then classifies people from 0 ("less prosperous") to 100 ("more prosperous"), a score that is used to guide the administration of social benefits. SISBÉN's clauses indicate that "the refusal to supply all the information requested will prevent your registration in SISBÉN" and that "any alleged falsehood identified through database cross-checks will generate exclusion from SISBÉN" as well as legal and judicial actions.[32] Since the program is designed to determine who is "truly" poor and thus "deserving" of social benefits, the provision of welfare benefits to a given individual is predicated on the complete and accurate collection of their requested data. With the objective of increasing efficiency in the distribution of benefits, digitized welfare systems focus primarily on identifying "liars" and "gate-crashers" rather than promoting inclusion of historically excluded groups.[33]

Such digital welfare systems mask several politicized assumptions under a veneer of objectivity. Their design is embedded with neoliberal fears of the "undeserving poor" but appear like "an objective examination of cutting-edge technologies." The Digital Welfare State risks treating poverty as an individual problem rather than a historical and systemic one[34]: for example, "SISBÉN narratives present issues of the State's inability to reduce poverty in recent years as a situation of a technical rather than a political nature. . . . not the effect of failing social policies but of the lack of a more modern and precise instrument that can 'search' for the 'real' poor." These new technological instruments also fit into a broader tradition of the State experimenting with economically vulnerable populations.[35] Viewing the Digital Welfare System as an objective assessment renders the data subject apolitical, thereby insidiously obfuscating the

[30] "Chased Away and Left to Die," *Center for Human Rights and Global Justice* (2021).
[31] "Identity."
[32] Joan López. "Experimenting with poverty" (2020).
[33] López.
[34] Varon and Peña.
[35] López.

oppression the data subject experiences. The subject appears to have rights over their data, but these rights become less meaningful when the power asymmetry and misalignment between data subject and data controller are so stark: the data subject aims to receive social benefits, and the data controller aims to keep out gate-crashers. Digital rights on paper should not mask the reality that the data subject and data controller operate on vastly unequal footing.

2.2. Consent[36]

An individualistic idea of consent and universalistic notion of public interest can combine to perpetuate oppression–governments implementing automated anti-poverty programs need either consent to access a poor person's data or a public interest exception to consent. Moreover, systems like SISBÉN garner consent for data collection by threatening to deny welfare benefits.[37] Another example is the Chilean program Alerta Niñez, which uses data about children and adolescents to measure risk of rights violations. Alerta Niñez predicates social benefits on data collection without providing individuals with clear information about the purpose or usage of their personal data. Alerta Niñez also discourages people from refusing consent with language like "We have made this decision as a family, in full knowledge of the potential benefits of this service" in sample rejection letters. Those in poverty do not have the free choice to say "no" when their welfare benefits rely on assenting to data extraction. Thus, this façade of digital consent has actually "been enabling a continuation of practices of (digital) colonialism embedded in cutting-edge digital technology and technosolutionist narratives focusing on maintaining the status quo." In data colonialism, "companies use long and incomprehensible documents, such as Terms of Service, as a form of power . . . to inescapably embed subjects in colonizing relationships."[38] Consent has been both implicitly forced and binary–the choice is all or nothing–and therefore not meaningful.[39]

An analytical definition of consent consists of the following four elements: freedom and "choice eligibility," knowledge of what you're consenting to, intention to consent, and ability to communicate consent.[40] Feminist thought suggests that consent is "a structural problem that is experienced at an individual level," rather than a subject making a "free, rational, and individual choice." Feminist scholars ask not only whether consent was given or not, but also whether it was even *possible* to give consent under the specific circumstances; structural factors influence all four elements of the analytical definition of consent. No means no, and a yes resulting from lacking the power to say no does not mean yes. The Feminist Data Manifest-No, a declaration that "refuses harmful data regimes and commits to new data futures," emphasizes this: "Not everyone can safely refuse or opt out without consequence or further harm. We commit to 'no' being a real option in all online interactions with data-driven products and platforms and to enacting a new type of data regime that knits the 'no' into its fabric."[41]

Meaningfully extending existing rights to vulnerable groups necessarily involves investigating the power structures of their specific situations, which requires a structural and collective understanding of consent. It's possible affirmative consent does not go far enough; while of course absolutely necessary, affirmative consent may foreclose further investigation of

[36] Varon and Peña.
[37] López.
[38] Varon and Peña.
[39] Varon and Peña.
[40] Feedback from Professor Alison McQueen.
[41] "Feminist Data Manifest-No."

the power hierarchies that made consent a necessity in the first place.[42] If we view Digital Welfare Systems as objective, we view the data subjects as apolitical, and their consent then serves to legitimize the politicized ideas that poverty is an individual problem and that welfare benefits need to be gatekept from undeserving liars. My point is not to do away with consent. I am arguing instead for the importance of viewing the data subject as politically constituted by interlocking power structures, in order to harness the full potential of the right to meaningful consent, and to understand the asymmetries between data subject and data controller that remain even after affirmative consent is given. Centering our consent conversations on power hierarchies can help us construct a more inclusive data subject, but an implicitly forced and binary form of consent risks reinforcing those hierarchies in the very name of data protection.

3. Vulnerability-aware Data Protection

The first statement in the Feminist Data Manifest-No reads: "We refuse to operate under the assumption that risk and harm associated with data practices can be bounded to mean the same thing for everyone, everywhere, at every time. We commit to acknowledging how historical and systemic patterns of violence and exploitation produce differential vulnerabilities for communities."[43] In this section, I show that reforming data protection must involve accounting for power asymmetries. Unlike other fields like consumer protection, data protection frameworks have "never really developed the notion of the data subject and the possible layers of data subjects in terms of awareness, understanding and weakness (e.g., the 'average data subject' versus the 'vulnerable data subjects')."[44] How can we reimagine the data subject to foreground power dynamics, to center the experiences of the most vulnerable members of society?

GDPR currently does not present an explicit definition of a vulnerable data subject, but it references vulnerability in recital 75 on Data Protection Impact Assessments: "where personal data of vulnerable natural persons, in particular of children, are processed." Recitals 38 and 58 explain that children deserve special protection because they may understand the risks less, and Recital 75 argues that special protection is required both in cases of limited capacity to give meaningful consent and of higher risks of damages. While GDPR does not explicitly extend this reasoning to other vulnerable adults–vulnerability on axes like race, gender, class, and sexual orientation remains relatively under-addressed–the possibility is left open. The Article 29 Working Party (WP29) response to GDPR states that a power imbalance defines vulnerability; WP29 lists children, employees, asylum seekers, the elderly, patients, and mentally ill persons as examples of vulnerable data subjects, along with "any case where an imbalance in the relationship between the position of the data subject and the controller can be identified." In Article 24 of GDPR, the data controller needs to analyze the risk level of the data subject before choosing the legal basis for data processing (consent or legitimate interests). The WP29 Opinion on legitimate interests calls for acknowledging "whether the data subject is an employee, a student, a patient, or whether there is otherwise an imbalance in the relationship" when data controllers determine if they want to process personal data based on legitimate interests. WP29 argues that it is important to note "whether the controller used 'knowledge of the vulnerabilities of the data subjects targeted.'" This risk-based approach in GDPR, which focuses on risks *during*

[42] Amia Srinivasan, *The Right to Sex* (London: Bloomsbury Publishing, 2021).
[43] "Feminist Data Manifest-No."
[44] Malgieri and Niklas.

and *because of* data processing, lends itself well to “a layered analysis of vulnerability, i.e. everyone is potentially vulnerable, but at different levels and in different contexts.”[45]

In order to address power dynamics in data subjecthood and thereby “unleash the GDPR potential in responding to particularly harmful practices that affect those in a disadvantaged position,” Gianclaudio Malgieri and Jedrzej Niklas propose a vulnerability-aware interpretation of data protection law, where vulnerability is defined as susceptibility to harm rather than the actual occurrence of harm. By centering on autonomy and integrity, power imbalance, and political and economic disadvantage, a vulnerability framework has the potential to challenge exclusionary assumptions within liberal individualism. At the theoretical level, there is a tension between the particularistic and universalistic character of vulnerability: Does focusing on specific groups as weaker or more vulnerable stigmatize them? On the other hand, does universalizing vulnerability gloss over the unique experiences of different groups? Additionally, there are two types of vulnerability risks–decisional vulnerability during data processing, such as the capacity to consent, and the harms created by data-driven systems, such as discrimination and manipulation. Focusing on harms can generate a list of damages that do not provide additional safety, but focusing primarily on procedural safeguards runs the risk of dismissing the reality of damage and suffering.[46]

One proposal to address these tensions of both definition and manifestation, Malgieri and Niklas argue, is layered vulnerability, where layers are “features constructed by status, time and location”; layering enables “a more intersectional approach and stresses its cumulative and transitory potential.” Layered vulnerability reconciles the universal and particular by showing that “all individuals are vulnerable, . . . but some individuals have more layers of vulnerability than others” due to “different social contexts and relational balances.” Under this framework, legal protection is proportional to the quantity and quality of layers, where layers are measured based on the origins and consequences of vulnerability, and mitigation strategies involve minimizing, eliminating, and avoiding the exacerbation of layers. A vulnerability-aware approach questions the rigidity of data subjecthood as currently conceptualized and acknowledges that data subjects lie on a spectrum of awareness, understanding, decisional capacity, and weakness.[47] Iris Marion Young writes that “[t]he varying and contradictory social contexts in which we live and interact, along with the multiplicity of our own group memberships and the multiple identities of others with whom we interact, make the heterogeneity of the subject inevitable.”[48] Layered vulnerability has the potential to aspire towards mainstreaming a heterogeneous, intersectional data subject.

In Articles 24 and 25 of GDPR, the data controller must prove their compliance with data protection principles and then implement them while taking into account “the risks of varying likelihood and severity for rights and freedoms of natural persons.” Drawing from the current understanding of vulnerable groups in EU law–across employment, biomedical research, public health, social assistance, and consumer rights–can help ensure that the data subject is inclusive of vulnerable segments of the population ranging from pregnant workers to visually impaired pedestrians to people affected by mental health disorders. Data Protection Impact Assessments–which involve describing data processing, assessing necessity and proportionality, and outlining measures to mitigate risks–can also account for vulnerability differences among

[45] Malgieri and Niklas.
[46] Malgieri and Niklas.
[47] Malgieri and Niklas.
[48] Young.

data subjects. In cases of clear power imbalance, consent may not be the best legal basis for data processing. For example, the European Data Protection Board Opinion on Clinical Trials states that consent should not be a legal basis for data processing when the data subject is in a situation of poor health conditions, socioeconomic disadvantage, or institutional or hierarchical dependency. Malgieri and Niklas qualify this claim by arguing that consent is only questionable in cases of decisional vulnerability and is recommended in other cases of vulnerability (such as risk of discrimination). Additionally, the rights of the data subject always take precedence over the legitimate interest of the data controller. Malgieri and Niklas also propose that data controllers can conduct periodic audits against discrimination when the data subjects come from historically marginalized groups. Lastly, sometimes the only path towards justice involves stopping the data processing altogether. The principles of fairness and lawfulness in Article 5(1) of GDPR can serve as barriers against data processing.[49]

However, these measures raise important questions. First, to what extent does this layered approach enable us to operationalize an understanding of universality as intersectionality? If the interaction of different layers represents interlocking structures of oppression, on what ethical foundation can we assign a relative weight to each layer, if at all? How do we think about the quality and quantity of layers with respect to different types of subjugation–such as structural, disciplinary, hegemonic, and interpersonal, the “matrix of domination” described by Patricia Hill Collins?[50] Second, do these measures place power disproportionately in the hands of the data controller to make arbitrary decisions regarding data subjects? To mitigate this, Malgieri and Niklas suggest codes of conduct and certification mechanisms for data controllers, but enforcing data-subject-centered behavior may prove challenging. If not the data controller, who should be responsible for assessing the level of vulnerability of a data subject? Design justice frameworks emphasize decision-making via community loci of power. As the Feminist Data Manifest-No states, “We refuse work about minoritized people. We commit to mobilizing data so that we are working with and for minoritized people in ways that are consensual, reciprocal, and that understand data as always co-constituted.”[51] Currently, Article 35(9) of GDPR states that “where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing,” and that the controller must justify their decisions to either not seek external views or disregard them. I argue that subverting power dynamics requires data subjects to be central participants in the design and technological process from the beginning, rather than “where appropriate.” Data protection agencies can also help provide recommendations on data processing for vulnerable groups.[52] Third, I wonder if the strategies motivated by higher levels of vulnerability should nevertheless be implemented across the board, rather than only when dealing with more vulnerable data subjects. What are the benefits and drawbacks of reimagining the entire foundation of data subjecthood for all data subjects, not just adding protections for the more vulnerable? Lastly, these measures are based on perceptions of who is most *at risk*, but perceptions of who *poses* the most risk are also often shaped by race, gender, and class[53]; how will data subjecthood account for this distinction?

Conclusion

[49] Malgieri and Niklas.

[50] Patricia Hill Collins, *Black Feminist Thought* (New York: Routledge, 2002).

[51] “Feminist Data Manifest-No.”

[52] Malgieri and Niklas.

[53] Theilen, 12.

In this paper I argue for the need to reimagine the data subject to acknowledge and subvert historical power dynamics. Viewing the data subject as an entity *with data to provide* and *with rights over that data*, I build on Aisha Kadiri's conception of the "paradox" of data protection, namely that a more inclusive data subject requires protection both *through* and *of* data. In Section 1, with the AfroZensus as a case study, I describe Kadiri's work on the bottom-up construction of a radically subjective, collective, and contextual data subject to advance racial justice. Aligning with Afrofuturist theory, understanding raw data as a function of power structures and empowering communities to take control of their data narratives are central to the creation of the data subject. In Section 2, I draw from Joana Varon and Paz Peña's analysis of Digital Welfare States to explore the dangers of assuming an apolitical data subject capable of making a meaningful choice despite an imbalanced playing field. I explore the importance of understanding structural asymmetries underlying the right to consent. Lastly, in Section 3, I discuss a layered-vulnerability approach, proposed by Gianclaudio Malgieri and Jedrzej Niklas, to redefining data subjecthood as more heterogeneous, intersectional, and inclusive in the context of GDPR. I consider their policy suggestions to acknowledge power dynamics, such as determining when consent is a relevant legal basis and when data processing needs to be stopped altogether.

For further research, I aim to flesh out the limitations of the layered-vulnerability approach and explore other alternatives. How can we transfer power from the hands of the data controllers to vulnerable communities, and consider how our perceptions of who *poses* the most risk factor into our understanding of data protection? I also hope to look into the idea of using human dignity as a constraint in data protection rather than solely as a means to empower autonomous individuals.[54] Additionally, I'm interested in exploring the promise and limitations of ideas like transparency and fairness in data protection discourse; some argue that these notions "function merely as a distraction" from the ways technology facilitates systemic oppression,[55] so I wonder to what extent they are valuable for the data subject and when they might stop being meaningful. As societal systems are increasingly digitized worldwide, it is crucial to ensure that our vision of who is represented in the data narrative and has meaningful rights over their data is inclusive and emancipatory. Without questioning status-quo assumptions, we risk embedding data protection discourse with historical power structures that harm the most vulnerable members of society.

[54] Anne de Hingh, "Some Reflections on Dignity," *German Law Journal* (2018).

[55] Theilen, 11.

Works Cited

"'Afrocensus' results: What is it like to be Black in Germany?" *dw*, www.dw.com/en/afrocensus-results-what-is-it-like-to-be-black-in-germany/a-59981987. Accessed 10 Feb. 2022.

"Afrozensus." afrozensus.de/. Accessed 10 Feb. 2022.

"Art. 4 GDPR: Definitions." *Intersoft Consulting*, gdpr-info.eu/art-4-gdpr/. Accessed 18 Jan. 2022.

Atrey, Shreya. "The Humans of Human Rights: From Universality to Intersectionality." *Intersectionality and Human Rights Law*, 22 February 2020, papers.ssrn.com/sol3/papers.cfm?abstract_id=3542773. Accessed 10 Mar. 2022.

"Chased Away and Left to Die." *Center for Human Rights and Global Justice,* 8 June 2021, chrgj.org/wp-content/uploads/2021/07/CHRGJ-Report-Chased-Away-and-Left-to-Die.pdf. Accessed 5 Mar. 2022.

Collins, Patricia Hill. *Black Feminist Thought: Knowledge, Consciousness, and the Politics of Empowerment*. New York: Routledge, 2002.

de Hingh, Anne. "Some Reflections on Dignity as an Alternative Legal Concept in Data Protection Regulation." *German Law Journal* 19, no. 5 (2018): 1269–90, doi:10.1017/S2071832200023038. Accessed 5 Mar. 2022.

Desai, Vyjayanti T., Anna Diofasi and Jing Lu. "The global identification challenge: Who are the 1 billion people without proof of identity?" *World Bank Blogs*, 25 April 2018, blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity. Accessed 5 Mar. 2022.

"Feminist Data Manifest-No." www.manifestno.com/. Accessed 16 February 2022.

Haraway, Donna. "Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective." *Feminist Studies* 14, no. 3 (1988): 575–99. doi.org/10.2307/3178066. Accessed 20 Dec. 2021.

"Identity in a Digital World: A new chapter in the social contract." *World Economic Forum*, September 2018, www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf. Accessed 5 Mar. 2022.

Kadiri, Aisha P.L. "Data and Afrofuturism: an emancipated subject?" *Internet Policy Review*, 7 December 2021, policyreview.info/articles/analysis/data-and-afrofuturism-emancipated-subject. Accessed 25 Jan. 2022.

López, Joan. "Experimenting with poverty: The SISBEN and data analytics projects in Colombia." February 2020. www.researchgate.net/publication/351699844_Experimenting_with_poverty_The_SISBEN_and_data_analytics_projects_in_Colombia. Accessed 10 Feb. 2022.

Malgieri, Gianclaudio, and Jędrzej Niklas. "Vulnerable Data Subjects," *Computer Law & Security Review* 37 (2020), doi.org/10.1016/j.clsr.2020.105415. Accessed 10 Feb. 2022.

Mohdin, Aamna. "Statistically speaking, black people in Germany don't exist." *Quartz*, 23 September 2017, https://qz.com/1078032/can-germany-combat-inequality-when-it-has-no-data-on-race/. Accessed 10 Feb. 2022.

Okin, Susan Moller. *Justice, Gender, and the Family*. New York: Basic Books, Inc., Publishers, 1989.

Okobi, Ekene. "The AfroZensus is an effort to quantify Blackness in Germany." *The World*, 10 May 2021, theworld.org/stories/2021-05-10/afrozensus-effort-quantify-blackness-berlin. Accessed 10 Feb. 2022.

Oltermann, Philip. "France and Germany urged to rethink reluctance to gather ethnicity data." *The Guardian*, 16 Jun 2020, www.theguardian.com/world/2020/jun/16/france-and-germany-urged-to-rethink-reluctance-to-gather-ethnicity-data. Accessed 10 Feb. 2022.

Perez, Caroline Criado. *Invisible Women: Data Bias in a World Designed for Men.* New York: Vintage Books, 7 March 2019.

Rogowska-Stangret, Monika. "Situated Knowledges." *New Materialism*, 2018, newmaterialism.eu/almanac/s/situated-knowledges.html. Accessed 20 Dec. 2021.

Srinivasan, Amia. *The Right to Sex: Feminism in the Twenty-First Century*. London: Bloomsbury Publishing, 2021.

Theilen, Jens T., Andreas Baur, Felix Bieker, Regina Ammicht Quinn, Marit Hansen, Gloria González Fuster. "Feminist data protection." *Internet Policy Review*, 7 December 2021, policyreview.info/articles/analysis/feminist-data-protection-introduction. Accessed 25 Jan. 2022.

Varon, Joana, and Paz Peña. "Artificial intelligence and consent: a feminist anti-colonial critique." *Internet Policy Review*, 7 December 2021, policyreview.info/articles/analysis/artificial-intelligence-and-consent-feminist-anti-colonial-critique. Accessed 25 Jan. 2022.

Young, Iris Marion. *Justice and the Politics of Difference*. Princeton University Press, 2011.