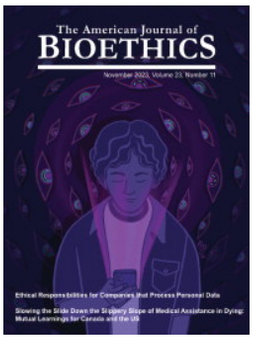

The American Journal of Bioethics

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/uajb20

Beyond Individual Rights: How Data Solidarity Gives People Meaningful Control over Data

Barbara Prainsack & Seliem El-Sayed

To cite this article: Barbara Prainsack & Seliem El-Sayed (2023) Beyond Individual Rights: How Data Solidarity Gives People Meaningful Control over Data, The American Journal of Bioethics, 23:11, 36-39, DOI: 10.1080/15265161.2023.2256267

To link to this article: https://doi.org/10.1080/15265161.2023.2256267

THE AMERICAN JOURNAL OF BIOETHICS
2023, VOL. 23, NO. 11, 36–39
https://doi.org/10.1080/15265161.2023.2256267

Taylor & Francis
Taylor & Francis Group

OPEN PEER COMMENTARIES

Beyond Individual Rights: How Data Solidarity Gives People Meaningful Control over Data

Barbara Prainsack and Seliem El-Sayed

University of Vienna

In today's digital societies, it has become very difficult for people to exercise meaningful control over what and how data is collected and used. McCoy and colleagues (2023) seek to address this problem by proposing an ethical framework that combines substantive and procedural principles, as well as factors needed for successful implementation. The Ethical Data Practices Framework (EDP) seeks to improve upon current data protection paradigms by overcoming the narrow focus on individual autonomy and pledging to uphold a set of relevant ethical principles.

While helpful in many regards, EDP leaves a few issues unaddressed. Solidarity-based data governance (in short: data solidarity; Prainsack et al. 2022a, 2022b), we argue, offers a solution to the very problem foregrounded by McCoy and colleagues, while also filling some of the gaps that the EDP leaves open.

WHAT IS DATA SOLIDARITY?

Data solidarity argues that the predominant Western approach to try to address power asymmetries by giving people more control over their data at the individual level is insufficient to solve structural problems. This instead requires strengthening collective forms of control, responsibility, and oversight (Prainsack et al. 2022a, 2022b).

The three pillars of data solidarity contribute to achieving this goal (Table 1). Pillar I comprises instruments and measures that facilitate data use that is likely to create significant public benefit without exposing individuals or groups to undue risks. To measure public value—a composite of benefits and risks—we also developed an online tool, the **P**ublic Va**LU**e Assessment **TO**ol (to be launched in October 2023; see below for details). The second pillar focuses on preventing and—where unsuccessful or impossible—mitigating harm from data use. Finally, Pillar III's goal is to guarantee that a fair portion of profits resulting from commercial data usage is given back to the people and communities that made the data use possible in the first place, e.g., by funding or creating data, infrastructures, or technologies. Cutting across these pillars is the fundamental tenet of considering and measuring the public value created by any given data *use*, rather than assuming that benefits and harms are tied to different data *types*.

FILLING EDP'S GAPS WITH DATA SOLIDARITY

Let us start by identifying the multiple points where McCoy and colleagues' approach aligns with data solidarity. EDP is rooted in three substantive and three procedural principles (see Table 1). The substantive principles are minimizing harm, fairly distributing benefits and burdens, and respecting individual autonomy. The three procedural principles are transparency, accountability, and inclusion.

Minimizing harm, and fairly distributing of benefits and burdens correspond closely with data solidarity. Transparency, accountability, and inclusion are inherent in the data solidarity approach as part of each of the three pillars (see Prainsack et al. 2022b for elaboration).

Two principles set the two approaches apart (Table 2; bold font). First, the concept of individual autonomy, a core tenet of EDP, is not explicitly outlined as a principle of data solidarity. Second, data solidarity's goal of facilitating data use that is likely to

CONTACT Barbara Prainsack barbara.prainsack@univie.ac.at Department of Political Science, University of Vienna, Vienna, Austria.

Table 1. Three pillars of solidarity-based data governance (source: authors).

Pillar I	Facilitate data use that creates significant public value
Pillar II	Prevent (or mitigate) harm
Pillar III	Bring some financial profits emerging from data use back to the public domain

create significant public value (Pillar I) is not reflected in EDP.

Respecting Individual Autonomy

Also for data solidarity, respecting individual autonomy is an important goal—but it is not listed as an explicit principle. Next to respecting individual autonomy—e.g., by not letting a vague notion of the "public interest" trump individual autonomy—data solidarity places strong emphasis on collective control over data use. The latter does not counteract personal autonomy, but rather enhances it. Going beyond Western individualism, data solidarity comprises wider forms of autonomy, recognizing that people are not only individuals but always also part of collectives.

Facilitating Data Use That Is Likely to Create Significant Public Value

EDP fails to address data harms that come from data use by any other than private companies. This, we believe, is due to two false assumptions that the authors adopted into their framework: Namely that (a) data use by for-profit companies should be *prima facie* treated differently from data use by other entities, and (b) that risk is inherent in data *types*.

McCoy and colleagues write that private commercial companies "warrant special attention due to their distinctive incentives and regulatory environment" (5). We contend that the nature or extent of any given data harm does not come (exclusively) from *who* is using the data. Although it is true that, as McCoy and colleagues argue, "government agencies and academic institutions have mandates to act in the public interest" (5), there are plenty of examples of public data use having created significant harm. In the US, algorithmic discrimination in public administration has disadvantaged ethnic minorities and women (Eubanks 2018; Richardson, Schultz, and Crawford 2019). Other countries offer additional examples, with the Australian Robodebt and the Dutch childcare benefit scandal being among the most notorious (e.g., Carney 2019; Peeters and Widlak 2023). Data harms may, as can be seen here, very well emanate from the (mis)use of data by other than for-profit bodies.

Table 2. Principles of data ethics framework and data solidarity compared (source: authors).

Approach	Principles						
Ethical data practices framework(ED)		Minimizing harm	Fair distribution of benefits and burdens	**Respecting individual autonomy**	Transparency	Accountability	Inclusion
Data solidarity	**Facilitating beneficial data use (Pillar I)**	Preventing and mitigating harm (Pillar II)	Sharing commercial benefits with the public (Pillar III)		(Inherent in Pillars I, II, and III)	(Inherent in Pillars I, II, and III)	(Inherent in Pillars I, II, and III)

Our other concern lies in McCoy and colleagues' adherence to the data type assumption. They highlight that in the era of data linkage the differentiation between health data and non-health data cannot be meaningfully upheld. Yet, by maintaining the idea that personal data is riskier than non-personal data they ignore that pervasive data collection and the linkage of extensive data sets often enable the identification of a person from seemingly innocuous information (Fazlioglu 2019). Information may also be sensitive and personal in one context and not in another. Data solidarity encompasses a radical shift away from assuming that risks and benefits are associated with data *types* to seeing them as a property of data *use*. Depending on what a (public or private) entity plans to do with data, different rules should apply. If a data use likely creates significant public benefit and avoids undue risks, it should be facilitated. If a data use can be expected to benefit the public but also poses high risks, the risks must be reduced before it can go ahead. Profits from low-risk data use that only creates commercial value should be shared with communities that enabled that data use in the first place. Finally, when and where data use would create no significant public benefits yet poses high risks, it should be outlawed, along with the threat and cross-border enforcement of considerable fines.

PLUTO: SYNTHESIZING AND OPERATIONALIZING THE RELEVANT QUESTIONS

In contrast to the EDP, data solidarity focuses on the public value that different types of data use create. To measure public value, the data solidarity team created PLUTO—a **P**ublic Va**LU**e Assessment **TO**ol (El-Sayed and Prainsack 2022). It offers a departure from the inflexible approach advocated by McCoy and colleagues, where the user's identity, whether public or private, is a decisive factor. Instead, PLUTO considers and weighs the status of the data user only as one of many factors that contribute to the likely public value of data use. PLUTO also includes questions about the benefits and risks pertaining to a given data use, as well as about the institutional safeguards in place.

PLUTO is not supposed to answer the question of the public value of different types of data use once and for all; in contrast, it is meant to facilitate a transparent and nuanced debate about how public value should be understood in the context of digital practices, and how it can be measured. The tool will be available open access and can be amended as needed by different communities and organizations.

CONCLUSION

McCoy and colleagues address the highly timely problem of people having lost, in most contexts, meaningful control over how data is collected and used. Their solution—the EDP—is a welcome contribution to solving this problem. Its strengths include the combination of substantive and procedural principles, as well as a consideration of factors needed for successful implementation. At the same time, it has drawbacks that include anachronistic assumptions about different levels of risk inherent in data types, as well as the uncritical continuation of a Western focus on individual-level solutions to collective problems. Data solidarity provides a solution to the lack of meaningful control over data while avoiding the drawbacks of the EDP.

ACKNOWLEDGEMENTS

The authors acknowledge the support of the Digitize! project at the University of Vienna, and The Lancet and Financial Times Commission on 'Governing health futures 2030: Growing up in a digital world'

DISCLOSURE STATEMENT

No potential conflict of interest was reported by the author(s).

FUNDING

The author(s) reported there is no funding associated with the work featured in this article.

ORCID

Barbara Prainsack http://orcid.org/0000-0002-6335-1532
Seliem El-Sayed http://orcid.org/0000-0003-4819-1136

REFERENCES

Carney, T. 2019. Robo-debt illegality: The seven veils of failed guarantees of the rule of law? *Alternative Law Journal* 44 (1):4–10. doi:10.1177/1037969X18815913.

El-Sayed, S., and B. Prainsack. 2022. Success of the European Health Data Space hinges on operationalizing public value, in addition to bridging digital divides. *BMJ Rapid Response* 378:e071913.

Eubanks, V. 2018. *Automating inequality: How high-tech tools profile, police, and punish the poor*. New York: St. Martin's Press.

Fazlioglu, M. 2019. Beyond the nature of data: Obstacles to protecting sensitive information in the European Union and the United States. *Fordham Urban Law Journal* 46:271.

McCoy, M. S., A. L. Allen, K. Kopp, M. M. Mello, D. J. Patil, P. Ossorio, S. Joffe, and E. J. Emanuel. 2023. Ethical responsibilities for companies that process personal data. *The American Journal of Bioethics* 23 (11):11–23. doi:10.1080/15265161.2023.2209535.

Peeters, R., and A. C. Widlak. 2023. Administrative exclusion in the infrastructure-level bureaucracy: The case of the Dutch daycare benefit scandal. *Public Administration Review* 83 (4):863–77. doi:10.1111/puar.13615.

Prainsack, B., S. El-Sayed, N. Forgó, Ł. Szoszkiewicz, and P. Baumer. 2022a. Data solidarity: A blueprint for governing health futures. *The Lancet. Digital Health* 4 (11):e773–e74. doi:10.1016/S2589-7500(22)00189-3.

Prainsack, B., S. El-Sayed, N. Forgó, Ł. Szoszkiewicz, and P. Baumer. 2022b. White paper: Data solidarity. *The Lancet & Financial Times Commission: Governing Health Futures*. https://www.governinghealthfutures2030.org/wp-content/uploads/2022/12/DataSolidarity.pdf.

Richardson, R., J. M. Schultz, and K. Crawford. 2019. Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. *NYUL Review Online* 94:15.

THE AMERICAN JOURNAL OF BIOETHICS
2023, VOL. 23, NO. 11, 39–41
https://doi.org/10.1080/15265161.2023.2256293

OPEN PEER COMMENTARIES

The Limits of a Voluntary Framework in an Unethical Data Ecosystem

Leah R. Fowler[a], Anya E. R. Prince[b], and Michael R. Ulrich[c]

[a]University of Houston Law Center; [b]University of Iowa; [c]Boston University

The need for greater privacy protections in the United States has never been greater. In their work, "Ethical Responsibilities for Companies That Process Personal Data", McCoy et al. (2023) correctly conclude that existing privacy laws and data protections are insufficient. Their proposed framework is an important scholarly contribution. We agree with their ideas about the practical imperatives, principles, recommended actions, and the promise of this work to inform policy. However, we worry that an emphasis on industry self-regulation could detract from full-throated advocacy for strong privacy legislation. Companies have collected and monetized personal data for years, not simply because they do not understand the ethical questions these practices raise or because they require better definitions. We believe the bioethics community must make legislative and regulatory change the primary focus for privacy protections. To support this position, we discuss the perverse economic incentives that may cause companies to advertise privacy protections they do not actually offer, the information asymmetries and knowledge gaps that prevent people from taking personal privacy precautions, and how the practical realities of the data economy minimize the likelihood and impact of a small number of companies opting for meaningful change. We bolster these three arguments with examples involving reproductive data.

The demand for privacy protections is and has been high. A 2020 report showed that an overwhelming majority of Americans (93%) would switch to a company that prioritized data privacy, and over a third of Americans would pay more money to interact with companies that had increased privacy protections (Transcend 2020). Since then, the Supreme Court's 2022 decision in *Dobbs v. Jackson Women's Health Organization* brought into stark relief the potential dire consequences that can arise when an ethos of widespread data collection collides with a lack of privacy protections. The risks and fear created by *Dobbs* sent demand for reproductive data privacy soaring, lending additional credence to McCoy et al.'s argument that there is a significant market opportunity for companies to use their framework to capitalize on advertised ethical data practices. However, it also

CONTACT Anya E. R. Prince anya-prince@uiowa.edu College of Law, University of Iowa, Iowa City, IA, USA.