Data solidarity: a blueprint for governing health futures

We live in an era of inequalities, many of which are being increased by digital technologies. Moreover, as noted by the *Lancet* and *Financial Times* Commission, "business models based on data extraction, concentrations of power, and viral spread of misinformation and disinformation represent defining features of the current phase of digital transformations".[1] At the root of these problems lie corporate practices but also public policies that allow data processors to accrue profits at the cost of people and communities. Individuals harmed by data use often have no access to remedies, either because they cannot prove who and what caused the harm, or because no law was broken.[2]

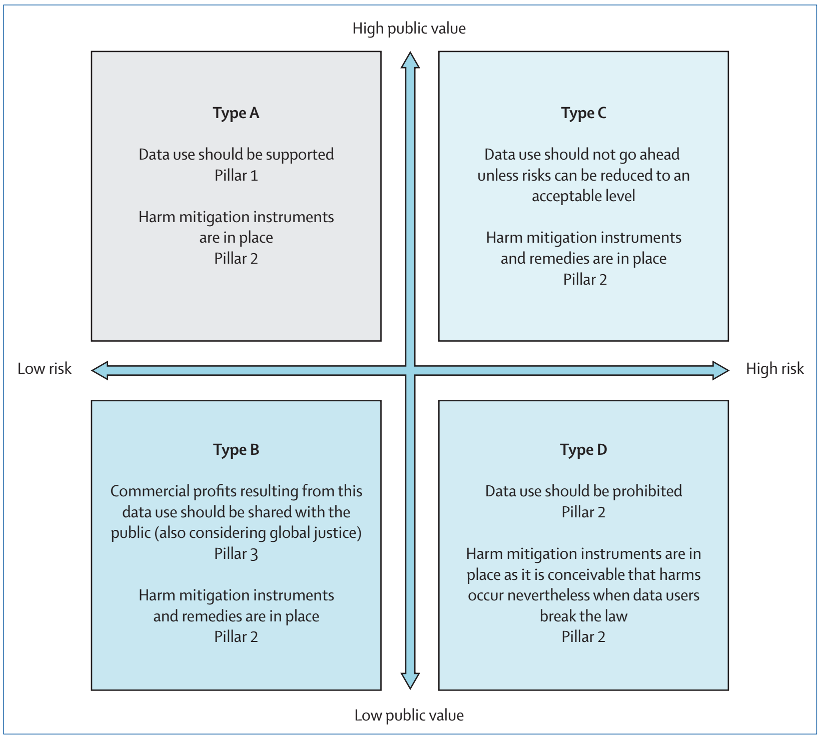
Against this backdrop, regulatory frameworks that seek to prevent harm mostly by strengthening the control that individuals have over their data are not enough. Although individual control is important, it cannot address the vast power asymmetries between data processors and data subjects. Neither does it respond to the fact that in the digital era, harm—just as benefits— can affect wider groups of people than only the primary data subjects from whom the data comes.

Solidarity-based data governance—by strengthening collective control and ownership of data—helps to ensure that the benefits and costs of digital practices are borne collectively and fairly. Next to preventing harm, data solidarity foregrounds the public value that specific instances of data use create. Data use creates public value when it benefits people and communities without posing grave risks (figure). Data use that creates little or no public value but poses substantial risks should be prohibited, with fines severe enough to deter even powerful corporations from breaking the law, and effective enforcement. Data use that poses no grave risks and is likely to benefit the public substantially, in contrast, should receive more public support (figure).

In this manner, data solidarity complements and helps to realise justice. It seeks to ensure that people are protected from harm, and proposes ways of owning, overseeing, and governing data beyond the individual-focused model.[3,4] It consists of three main pillars: facilitating good data use (pillar 1); preventing and mitigating harm (pillar 2); and returning profits to the public domain (pillar 3).

Data use that would create considerable public value—often in non-profit health research—can be very difficult or even impossible to carry out because regulation is unduly onerous, or due to financial, technological, or practical barriers. Data solidarity requires that such data uses receive more public support by removing red tape or by providing financial and practical assistance. Examples for how this could be done exist.[5,6]

Concerning data use that poses grave risks to individuals or communities, in contrast, data solidarity requires making use of the full force of the law to prohibit such harmful practices. For large corporate actors, the costs of breaking the law must be increased, such as by multiplying fines for repeat offenders and by improving cross-border cooperation in law enforcement. At the same time, some risks will remain, also in the case of beneficial data uses. When people are harmed by data use, they need remedies that are easily accessible and effective. One way to reach this goal is the creation of harm mitigation bodies at regional, national, or supranational level that would complement existing legal remedies.[2]



Type A

Data use should be supported
Pillar 1

Harm mitigation instruments are in place
Pillar 2

Type C

Data use should not go ahead unless risks can be reduced to an acceptable level

Harm mitigation instruments and remedies are in place
Pillar 2

Type B

Commercial profits resulting from this data use should be shared with the public (also considering global justice)
Pillar 3

Harm mitigation instruments and remedies are in place
Pillar 2

Type D

Data use should be prohibited
Pillar 2

Harm mitigation instruments are in place as it is conceivable that harms occur nevertheless when data users break the law
Pillar 2

Figure: **Four types of data use**

Where commercial profits accrue from data use, some of these profits need to come back to the people and communities that enabled them in the first place. The European Commission proposed corporate taxation specific to the digital economy[7] to be accompanied by a future global minimum corporate tax.[8] Corporate taxation for digital businesses could also help to reduce inequities between countries where digital businesses operate and where they pay taxes.[9] An additional way of giving the people and communities more collective control over the profits from data use are data commons, in which data and other digital resources are governed collaboratively, guided by the values of fairness, equality, justice, and sustainability.[10]

The benefits from digital data and technologies are considerable, but they are distributed unequally. At the same time, people and communities that bear the costs of data use are often left behind. Societies have a collective responsibility to ensure that digital practices help to improve the lives of all people, and that harms are prevented more effectively. Data solidarity provides a blueprint of how to make this happen.

We declare no competing interests.

We gratefully acknowledge the financial support for research assistance provided by *The Lancet* and *Financial Times* Commission on governing health futures 2030: growing up in a digital world.

**Barbara Prainsack, Seliem El-Sayed, Nikolaus Forgó, Łukasz Szoszkiewicz, Philipp Baumer*
barbara.prainsack@univie.ac.at

Research Platform Governance of Digital Practices (BP) and Department of Political Science (SE-S, PB), and Research Platform Governance of Digital Practices (NF), University of Vienna, Vienna 1010, Austria; Faculty of Law and Administration, Adam Mickiewicz University in Poznań, Poznań, Poland (LS)

1 Kickbusch I, Piselli D, Agrawal A, et al. The *Lancet* and *Financial Times* Commission on governing health futures 2030: growing up in a digital world. *The Lancet* 2021; **398:** 1727–76.

2 McMahon A, Buyx A, Prainsack B. Big data governance needs more collective responsibility: the role of harm mitigation in the governance of data use in medicine and beyond. *Med Law Rev* 2020; **28:** 155–82.

3 Kukutai T, Taylor J. Indigenous data sovereignty: toward an agenda. Canberra: ANU Press, 2016.

4 Braun M, Hummel P. Data justice and data solidarity. *Patterns* 2022; **3:** 100427.

5 Republic of South Africa. Protection of personal information act. 2013. https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf (accessed Oct 7, 2022).

6 Findata. A year in review — summary of Findata's operations in 2020. 2021. https://findata.fi/en/uutiset/a-year-in-review-summary-of-findatas-operations-in-2020 (accessed April 14, 2021).

7 European Commission. Proposal for a council directive on a 'digital levy'. 2021. https://op.europa.eu/en/publication-detail/-/publication/8f4d4f02-5676-11eb-b59f-01aa75ed71a1 (accessed Oct 7, 2022).

8 European Commission. Proposal for a council directive on ensuring a global minimum level of taxation for multinational groups in the union. 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0823&qid=1641150862839 (accessed Oct 7, 2022).

9 African Union. Taxing the Digital Economy: COVID-19 heightens need to expand resource mobilization base. 2020. https://au.int/sites/default/files/pressreleases/39159-pr-4th_high-level_policy_dialogue_pre-event_pr.pdf (accessed Aug 14, 2022).

10 Hicks J. The future of data ownership: an uncommon research agenda. *Sociol Rev* 2022; published online May 16. https://doi.org/10.1177/00380261221088120.