

In this together

Combining individual and
collective strategies to
confront data power



with support from



OMIDYAR NETWORK™



Summary

This think piece results from discussions between four advocacy organisations working to improve how data is governed. In our work, we have found that common ambiguities in how individuals, groups, rights, protections, control, and personal data are discussed can create the impression of advocacy groups pulling in different directions and working on separate agendas. However, by unpacking some of these concepts, we have sought to uncover the alignment, overlaps and connections between our work. We offer this piece primarily with the non-profit community in mind, in an effort to add clarity and complementarity to the advocacy efforts of organisations like ours. Specifically, in this paper, we argue that individual and collective approaches for data governance should be seen as complementary: both addressing particular challenges within the status quo.

Section one begins by setting out the challenges that come from confusion over key terms, and how ambiguity of language can lead to organisations with common cause being seen as at cross-purposes. Section two explores some of the terms that can trip us up, looking in detail at five different areas of conceptual and rhetorical ambiguity: suggesting key distinctions to make and questions to ask when designing advocacy strategies. Section three reflects on these distinctions, using them to map the data governance tools and approaches that are actually available to people and groups, and the limits of current mechanisms to challenge the status quo. The final section notes three insights:

1. Individual data protection rights are necessary but not sufficient to deliver better governance of data at scale.
2. Many group-based data governance approaches are strengthened by building on individual data protections.
3. Gaps remain in the data governance toolbox and require interlocking individual and collective governance mechanisms to fill them.

We close with recommendations for how the advocacy community can build on these insights to strengthen shared work towards a more fair data future.



Understanding the challenge

Power in the digital world is not equally distributed. Indeed, concentrations of capital and data increasingly impinge upon the freedom and autonomy of individuals and communities across the globe. Although it is common for debates to focus on totemic examples like the big social media, search and software companies, data power is exercised by all sorts of institutions, from local and national governments to banks, travel firms, and companies operating hidden away in the supply chain.

Since the 1980s, the articulation and implementation of individual data protection rights have gathered pace. All four of the modalities of regulation outlined by Lessig¹ have been explored to create the possibility of greater individual control over data: from the articulation of norms for fair information processing, to the creation and promulgation of data protection laws, the development of software architectures that support decentralised control of data, and articulating data ownership narratives to attempt to challenge the dominant market power of data-extractive firms.

Discussions of data governance² have often been dominated by the language of privacy and personal data protection. However, concerns have increasingly been raised about the sufficiency of frameworks focussed solely on individual data rights. Viljoen has pointed out how the relational nature of data³ creates challenges for ownership-based approaches to data control, and companies have been accused of co-opting a discourse of privacy norms to create privacy-theatre regimes of notice-and-consent that provide limited meaningful control for individuals.⁴ Data protection laws appear to have done little in practice to re-balance power between data subjects and data holders.

Concerns about the limitations of individual rights frameworks have led to work on how to secure the data rights of, and control over data for, groups and communities. Multiple advocacy initiatives and institutions have been launched, and numerous new structures for data control and governance have been proposed, from commons and co-operatives to trusts and unions.⁵ There is a host of theoretical and legal writing attempting to understand what is needed and what is feasible in

1 Lessig, Lawrence. Code: And other laws of cyberspace. 1999

2 We use the term “data governance” to refer to the ways in which decisions are made about how and whether data is collected, shared, analysed, and used in decision-making, in both policy and practice.

3 Viljoen, Salome. (2020). A Relational Theory of Data Governance, <http://dx.doi.org/10.2139/ssrn.3727562>

4 Waldman, Ari Ezra. Industry unbound: The inside story of privacy, data, and corporate power. Cambridge University Press, 2021.

5 For a mapping of organisations working in this space, see the Datasphere Atlas (2022) at <https://www.thedatasphere.org/programs/intelligence-hub/datasphere-governance-atlas/>.

terms of the collective governance of data.⁶

Too often, however, collective and individual arguments are framed in opposition to one another, with individual data rights and ownership on one side and arguments for collective governance of data on the other. This framing risks an adversarial approach, in which communities working to challenge the status quo through individual rights, and those working on collective governance, appear to be pulling in opposite directions. Instead, in this paper, we argue that individual and collective approaches for data governance should be seen as complementary: both addressing particular challenges within the status quo and aiming at responsibly unlock the value and benefits of data for all.

To show how, we first need to unpack what has become a quite messy discourse: with confusing overlap and ambiguity of ideas about various topics, including personal and non-personal data; the nature of groups and their formation; and the difference between the governance of collective data and the collective governance of data. The popular use of oversimplified analogies has contributed to confusion, - inhibiting the advocacy community's potential to leverage the complementary power of individual and collective rights, governance models, incentives, and opportunities.

This ambiguity represents an opportunity cost that the authors of this paper have experienced first-hand in various ways, inhibiting the empowerment and protection of people and groups. As advocacy organisations playing different roles, in varied geographies, and working with different configurations of stakeholders in this fast-developing space, we come to this essay because we have found ourselves heading in a common direction, yet through different lenses. We believe that meaningful deliberation can help to disambiguate apparent contradictions, thereby strengthening our independent and shared advocacy efforts. We need more careful thinking and measured distinctions to advance the different ways in which individuals and groups can take control over how their data is used and shared, and how those arrangements should benefit them instead of harming them.

- 6 Select examples include: Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, 49, 424–438. <https://doi.org/10.1016/j.IJINFORMGT.2019.07.008>; Asaf Lubin. (2023). Collective data rights and their possible abuse. *Temple Law Review*, 95(4). <https://www.templelawreview.org/essay/collective-data-rights-and-their-possible-abuse/>; Chapter 3-4 in Punia, S., Mohan, S., Kakkar, J. M., & Bhandari, V. (Eds.). (n.d.). *Emerging trends in data governance*. National Law University Delhi Press. Retrieved August 13, 2023, from <https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/nlu-delhi-law-book-2022-ff-web-345.pdf>; Viljoen, S. (2021). A Relational Theory of Data Governance. *Yale Law Journal*, 131(2), 573–654. <https://www.yalelawjournal.org/feature/a-relational-theory-of-data-governance>; Marcucci, S., Alarcón, N., Verhulst, S., & Wüllhorst, E. (2023). Informing the Global Data Future: Benchmarking Data Governance Frameworks. *Data & Policy*, 5, E30. <https://doi.org/10.1017/dap.2023.24>. See also Data Governance and the Datasphere Literature Review, by the The Datasphere Initiative Foundation. December 1, 2022.
- 7 De La Chapelle, B. and L. Porciuncula (2021). We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty. Internet and Jurisdiction Policy Network <https://www.internetjurisdiction.net/uploads/pdfs/We-Need-to-Talk-About-Data-Framing-the-Debate-Around-the-Free-Flow-of-Data-and-Data-Sovereignty-Report-2021.pdf>

This piece aims to contribute to that effort by sharpening several common concepts, and suggesting how the distinctions drawn can help us think about the digital society we are fighting for.



Clarifying concepts

This piece aims to contribute to that effort by sharpening several common concepts, and suggesting how the distinctions drawn can help us think about the digital society we are fighting for.

Personal and non-personal data

Personal data is sometimes defined as data that originates from or by individuals or their actions, and at other times defined as any data which can be associated with individuals (data from me, vs data about me).⁸ In other words, "data from me" is information actively provided

8 Data "From Me" refers to information that an individual voluntarily provides or generates. This data is actively shared by the data subject. It includes data that individuals intentionally submit or create, often as a result of their actions, choices, or interactions. Examples include: (a) Personal details provided when filling out a job application, online form, or social media profile. (b) Content and messages shared on social media platforms or via email. (c) Preferences and settings chosen on websites and apps, such as selecting favourite products or customising user profiles. (d) Data generated by wearables and smart devices, like fitness trackers or smart thermostats, based on user activity. Data "from me" is typically within the individual's control, and they have the ability to decide what information to share and with whom. Data "About Me" may include data "from me", but may also be collected, observed, or inferred by external entities, such as companies, organisations, or government agencies, without the active involvement of the data subject, often for the purposes of marketing, research, or service customization. This can include (a) Purchase history and browsing behaviour tracked by online retailers or advertisers. (b) Location data collected by mobile devices or apps, showing where the individual has been. (c) Health records maintained by healthcare providers and insurers. (d) Social media analytics data, including information about a person's online behaviour and interactions. Many data protection laws, including the GDPR and the California Consumer Privacy Act (CCPA), define personal data as data "about me".

or generated by the data subject, whereas "data about me" is information collected or inferred by external entities. These point to a conceptual distinction that helps in understanding the origin and control of personal data.

There are subtle and important differences between these two conceptualizations of personal data, particularly in terms of how individuals might be able to control each kind of ‘personal data’. However, both these definitions are problematic because they exclude many types of data with implications, associations, and consequences for human persons (data that impacts me).

Data from people might be considered ‘non-personal’ (no longer strictly about them) when it has been anonymized. Data protection mechanisms focused on individuals generally do not account for such dynamics, yet this type of data can nevertheless drive decision-making that directly affects people in very personal ways, impacting their access to healthcare, the types of political discourse they are exposed to, or policy and regulations with direct impacts on their daily lives, from the planning of urban transit to the access to social benefits.

Similarly, data that has not been created by, or even strictly about, individuals, such as satellite imagery, waste-water quality monitoring, or economic reports can have very personal consequences when used to make decisions on land rights, lockdowns, infrastructure development, or the local allocation of public resources. In this and other ways, so-called non-personal data can affect individuals and groups immediately and personally, if in a manner that is often opaque and difficult to discern.

Distinguishing between ‘data from me,’ ‘data about me’ and ‘data that impacts me’ is important because it highlights how ‘non-personal’ data is nevertheless personal. Even though these categories may overlap in practice or regulation, distinguishing between them highlights the different kinds of data protection strategies and tools that are available for each.

Data from me	Data about me	Data that impacts me
Data actively provided or generated by an individual.	Data that relates to an individual, but that was collected or inferred by a third party.	Data with implications, associations, and consequences for an individual.
Examples		
Social media posts; address information provided when signing up for a service; and data from a smart watch.	The inferred profile an advertiser creates; health records made by the doctor; and ratings of a gig worker.	Wastewater monitoring used to decide on health lockdowns; aggregate transport data used to plan transit infrastructure.



Collectives, communities and groups

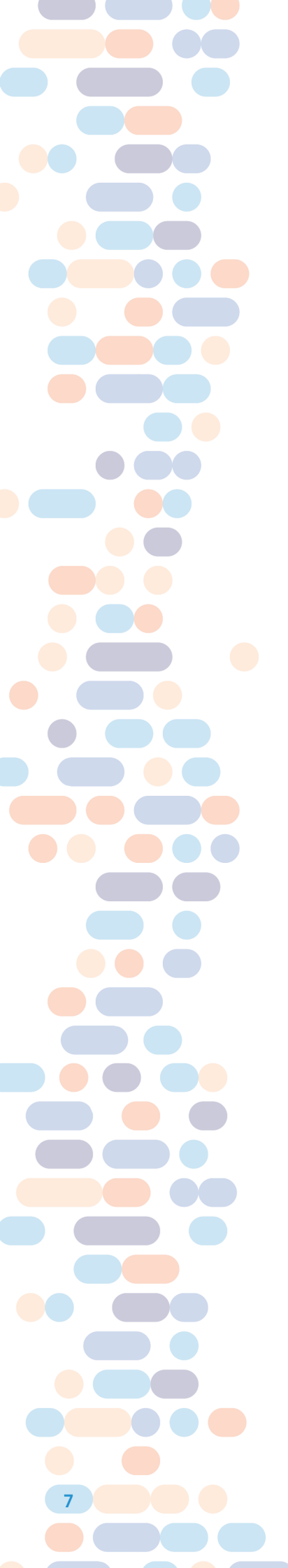
Recognising that the value of data often exists not at the level of individual records, but in the collection of data about, or impacting on, groups of individuals, there has been considerable focus in recent years on collective and community models of data governance. The terms ‘collective’ and ‘community’ are sometimes deployed with an explicit or implicit normative connotation, pointing to ideas of collective interest, or drawing on a positive ideal of community. To separate the normative from the descriptive, we find it useful to focus on groups in data governance and to look at how groups are defined by agency, purpose, and the grounds on which group rights are established.

Individual agency and group dynamics

Increasingly, the data-driven decisions that most affect us are not personal data associated only with us as individuals, but are based on groups in which we have been placed without our knowledge: amalgamations of our collective consumption behaviours, mobility patterns, communication, and demographics. We can call these “automatic groups”, and we can distinguish them from what we might call “express groups”, which are formed deliberately. People explicitly and deliberately join political parties and labour unions, they enrol in patient-driven health research, they join online forums and support groups set up for people just like them, and social media platforms for all types of people.

Automatic groups	Express groups
A group that individuals are placed into by a third party without their direct action, and on the basis of some collection of data points or features.	A group that an individual voluntarily opts in to join through some express action.
Examples	
Marketing categories; people in health records with a given configuration of symptoms; people with particular travel patterns.	Labour unions, political parties, online forums, social media groups etc.

However, even when an individual decides to join an “express group”, their data might end up being collected and used to form an “automatic group”. Data on social media groups and communities is for example often aggregated, compared, used in decision-making, and sometimes sold or shared with third parties.

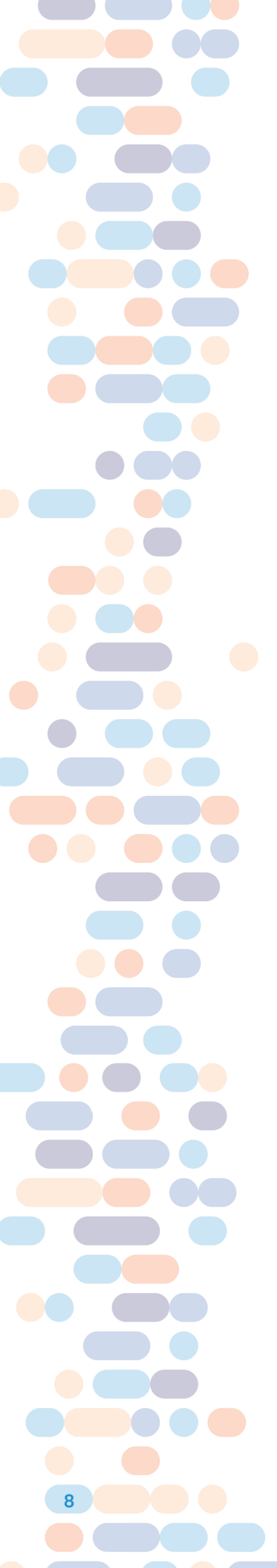


Group purpose and data focus

The distinction between automatic and opt-in express groups is intuitive, but more nuanced than it first appears. There are different degrees of awareness and agency involved in joining a group. Between the extremes of unknowingly being placed in a dataset, to actively joining an initiative so that it can use people's data for their benefit, there are the grey zones: you may know that you belong to a group that you did not actively join, such as your neighbourhood or tax bracket; you may know that you are joining a data group by signing up for an online service, but not know what it implies; you may join a group like a homeowners' association because you had no pragmatic option to decline membership.

In this context, the motivations driving group participation and the objectives of these groups carry significant weight. Lately, various express groups have been exploring the establishment of legal or organisational frameworks, such as data trusts, cooperatives, stewardship, and collective governance structures, all with the explicit aim of safeguarding and empowering their members by influencing the management and utilisation of their data. The choice to join a collective focused on health data sharing for medical research, even when anonymized, differs substantially from becoming a member of a car-sharing group or a frequent fliers club. This is because despite the similarity in the effort required for joining and the potential for each to impact how their data is collected, utilised, and shared externally the intent for joining each group is very different. The goals of these organised groups and the level of active involvement from their members also align with their ability and potential to proactively govern their data, particularly in response to potential harm or misuse.

Data as a primary focus	Data as a secondary focus
Groups formed or joined with the explicit goal of exercising control over data.	Groups formed or joined that can exercise some control over data, but where this is more-or-less incidental to the groups main purpose.
Examples	
Health data sharing co-operative. Energy data trust. Data-focussed campaign group.	Car sharing group. Frequent fliers club.



Grounds for group rights

The purposes and the motivations of groups can also influence the justifications for groups' data rights and governance strategies, and we can distinguish between two main theoretical premises for vesting data rights in groups:¹⁰

(a) The Choice Theory, where group rights primarily serve as an aggregation of individual values, providing a choice to holders in exercising their rights.¹¹ Key features of choice theory include: individual autonomy, aggregation of interests, exercise of individual rights, protection of minority interests to ensure that even minority views and preferences are considered in group decision-making.

(b) The Interest Theory, which places greater emphasis on safeguarding collective interests that may extend beyond the mere aggregation of individual interests, thus emphasising the implicit moral imperative to safeguard collective interests that may be more than the aggregated interests of its individual members.¹² Key features of interest theory include collective interests that are unique and independent from individuals, a moral imperative to protect and promote the interests of the group as a whole, the balancing of interests and prioritisation of the broader group interests and identity above those of the individual.

Viewing group rights from the lens of the choice theory resonates with market-driven paradigms, where the aggregation of individual preferences and actions forms the basis for determining group outcomes. In the community data context, this theory underscores the idea that collective rights emerge as a natural consequence of individual contributions, ensuring that each participant's voice is accounted for in the group's decision-making.

On the other hand, interest theory introduces a moral dimension to the discussion of group rights. Here, the interests of a group take on a separate identity that holds a broader moral significance than combined individual concerns alone. The interest theory acknowledges the implicit moral responsibility to safeguard this collective well-being, accounting for the power dynamics within interconnected digital networks that may disproportionately impact certain groups.

10 Preda, A. (2015). Rights: Concept and Justification, *Ratio Juris*, 28: 408–415, <https://doi.org/10.1111/raju.12090>

11 De George, R. T. (1987). Review of Collective and Corporate Responsibility., by P. French, *Noûs*, 21(3), 448–450, <https://doi.org/10.2307/2215198>

12 Ruben, D. H. (2008). Review of The Reality of Social Groups, by P. Sheehy, *Mind*, 117(467), 731–735, <http://www.jstor.org/stable/30166335>

Importantly, the two rationales do not stem directly from groups’ purposes or the agency with which they are formed as express or automatic. They instead provide a third distinction that we believe can be helpful for thinking about different types of groups in data advocacy strategies.

What defines a group?	
Agency	Are groups express (I decided to join) or automatic (I was added to it)?
Purpose	Are groups joined or formed specifically in order to affect how data is governed?
Grounds for group rights	Are the rights associated with the group reducible to the sum of the rights of the individual members or is the group a subject of rights beyond the sum of the rights of its individual members?

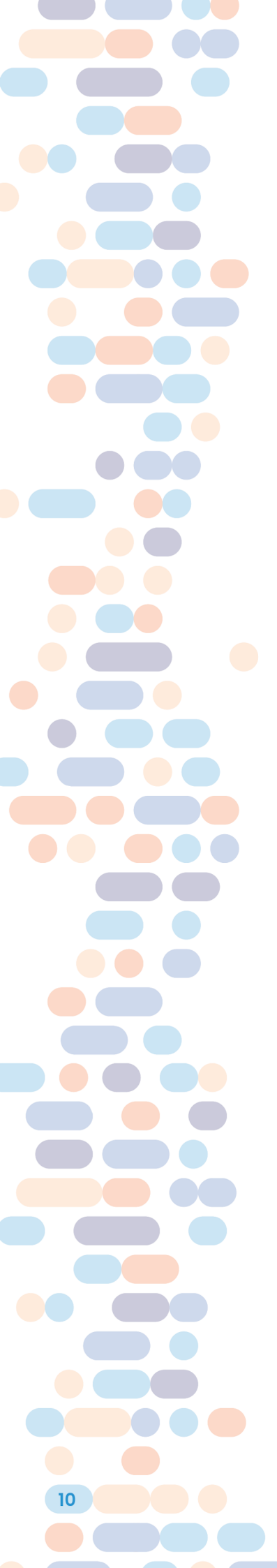
These three dimensions present in the table above are by no means exhaustive. Many other distinctions could be made, and there is a burgeoning literature on group rights and data rights that suggests several useful ways to think about different kinds of groups and their consequences. We nevertheless believe that these three distinctions are particularly helpful for tactical thinking and that answering these questions in the design of advocacy strategies can strengthen their legitimacy and impact.

Control, consent and agency

When we think about how individual and group-based strategies are deployed to govern data, we can distinguish between ‘taking back data’ and ‘taking back control’.

Individuals may use data protection or human rights legislation to demand that third parties collect, process or delete data in fair ways. Similarly, groups might mobilise to advocate for companies, institutions or industries to change their data governance practices or to make concessions to community demands. If successful, these are instances in which individuals and groups take back control over how their data is used.

Other approaches might go further than exercising influence or control, and seek to take back de jure or de facto ownership of data. Decentralised technologies, personal data stores, and data trusts or cooperatives are all means of taking back data. That is, structurally relocating data or copies of data from centralised datasets owned and controlled by third parties (often corporations or governments) into databases owned or controlled by the individual, or by an organised



group of individuals who have come together to create their own data-holding structures.

All of these approaches face significant challenges. Both taking back control, and taking back data, frequently require some level of technical capacity, as well as the time and resources to engage more directly with questions of how data is, or should be, managed. Efforts to take back control by securing agreements or concessions from large data-using organisations are only effective if those organisations actually honour and implement commitments, and it can be difficult without solutions either in code or through regulatory action, to secure the oversight needed to make sure this is happening. Many technical solutions to take control of data directly involve taking a copy but do not prevent third parties from maintaining and using their own copy of that data as they see fit.

It is also worth noting that any efforts made by groups to proactively govern data, or seek redress for data misuse, will likely be implemented through a principal-agent relationship, in which members of the group empower others to act on their behalf. This mechanism has great potential to strengthen individuals' limited capacity and expertise to take control over data governance, and this is often the entire point of stewardship models like data cooperatives, collectives, or trusts. Such groups remain prone to some of the other challenges that often plague governance in principal-agent relationships, however, such as compounded information asymmetries, the deviation of interests over time, and adequately funding fiduciaries. There are also potential legal challenges. The EU Data Governance Act, for example, notes that the rights from the GDPR can only be exercised by an individual and cannot be conferred or delegated by them to another party, such as a data cooperative, thereby limiting any exercise of data protection rights by agents on behalf of principals.¹³

A distinction can also be made between the capacity of individuals and the capacity of groups to exercise control over their data before that data has been accessed by a secondary or third party. This type of control is most usually exercised by mechanisms of consent, which for individuals is often limited by skewed incentives and insufficient information, knowledge, or expertise if consent is even legally required or requested in the first place. Group consent, on the other hand, is generally not recognized as a requirement for data processing or use, though data collectives and stewards may be able to demand consent if they have exclusive control over valuable data. In such cases, it can be argued that the use of group data be based on a legitimate interest defined in dialogue with groups.

The capacity of groups and individuals to exercise control over their data is most obvious in regard to the legal basis for individuals' data protection and privacy rights for individuals. Codification of those rights does not guarantee them, however, and there are multiple factors influencing the capacities of both individuals and

13 See <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767>, Recital 24.

groups to take control over their data, at the point of its creation, use, or in redress.

Questions about meaningful control	
Control vs storage	Do people need to host and have exclusive control over their data in order to control how it is used? What are the limitations to control through storage?
Prior consent	What options can be exercised to assert control over data before it is used or processed? What factors limit the ability of individuals and groups to demand consent or other legal justifications for data use?
Principal vs agent	Do the limitations on individuals' capacity for control or consent suggest the need for representation by an agent? What are the practical and legal obstacles and opportunities?

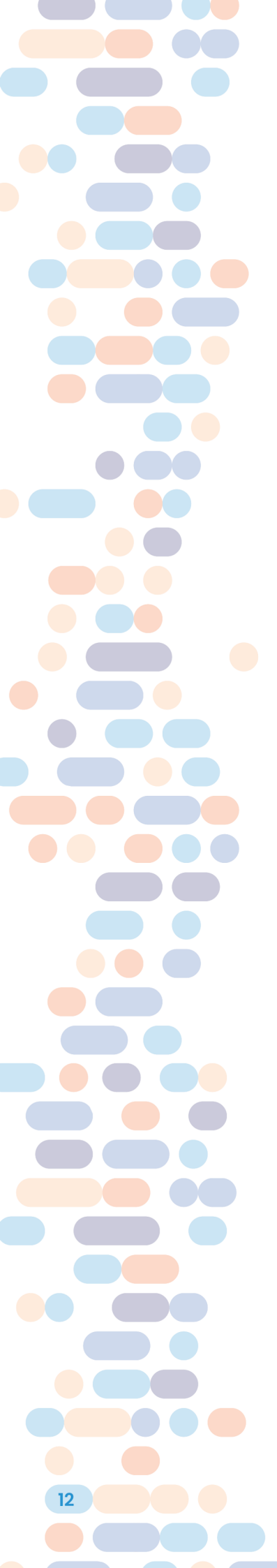
Rights and their legal foundations

Advocacy commonly references the idea of data rights, referring both to individual and collective rights to control and agency over data. However, the legal foundations for these different kinds of rights are developed to different degrees, and where the former may frequently involve reference to established legislation, the latter often involves a set of normative claims rather than invocation of codified law.

The privacy and data protection rights of individuals are clearly established in landmark legislation such as the EU's GDPR, the Brazilian data protection law (LGPD), and other national regulatory frameworks around the world. While the GDPR and comparable regulations articulate multiple rights for individuals, it is unclear whether there are sufficient legal and practical mechanisms for individuals to easily and meaningfully exercise their formal rights to access, port, delete or otherwise seek redress for their data. This is particularly the case in many contexts where these rights are not well known. Nor is it clear that these rights are applicable for data based on automatic groups or de-anonymized data defined as non-personal data in specific regulations.

Increased awareness about the implications of co-generated and aggregated data on groups has prompted a discourse on groups' privacy and data rights, but there is little positive law establishing such rights as present. Though the EU Data Governance Act

14 For a detailed discussion in the UK regulatory context, see the forthcoming Connected By Data policy brief - https://docs.google.com/document/d/1kenOrkFWO4A7nfBd_2WB_rf8TA_QAtZwPII2Kvq5PaI/edit#heading=h.jgmduqp1336.



recognizes the importance of collective groups in its treatment of data altruism, that act explicitly restricts the rights it articulates to individuals.¹⁵ There have been some efforts to build collective digital rights on the basis of more traditional collective rights that are awarded to minority groups in some jurisdictions. A significant amount of work has been done across the world to bring legal collective actions on the basis of groups' data rights for example.¹⁶ International human rights law may also provide a basis for this through the collective rights to self-determination, language, collective identity, and other cultural rights.¹⁷ Early explorations of this potential have emphasised the mutually reinforcing nature of individual and group rights to privacy.¹⁸ The Indian Judiciary, for example, in examining the boundaries of a fundamental right to privacy, has explored the intersection of the general right to privacy with an individual's group-based identities, supporting the exercise of such identity characteristics through recognition of group privacy rights.¹⁹

While codified rights exist almost exclusively for individuals, there are a few examples of rights for groups. The UN Declaration on the Rights of Indigenous Peoples recognises the importance of maintaining cultural, linguistic, and religious identities within indigenous communities. Within the digital ecosystem, there is a growing discourse around indigenous data sovereignty ("IDS")²⁰ which refers to the right of indigenous peoples to control data from and about their lands and communities, both on an individual and collective level. IDS concerns itself with both electronically stored data as well as knowledge, meaning the scope is far broader than for traditional data governance frameworks. The Anti-Racism Data Act in British Columbia is one example, recognizing specific rights for "indigenous peoples" in the use and governance of data about them.²¹

Despite these early developments and foundations, group data rights have not been widely recognized in law or practice. This contrasts starkly with the proliferation of data protection regulations around the globe. Additionally, it would be a mistake to assert that

15 See <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0767>, Article 9 and preamble, respectively.

16 See for example this collection of lessons from the Digital Freedom Fund, <https://digitalfreedomfund.org/collective-redress-lessons-from-around-the-globe/>.

17 ICCPR references self determination loosely, ICESCR the others. Both are hard law, UN Decl' on Indigenous ppl's rights, has some customary and soft law force.

18 Linnet Taylor, Luciano Floridi, and Bart Van Der Sloot (eds.) Group Privacy: New Challenges of Data Technologies. Heidelberg: Springer International Publishing. See https://www.researchgate.net/publication/321537799_Group_Privacy_New_Challenges_of_Data_Technologies

19 Alevoor, S. (2022). Decisional Autonomy and Group Privacy – on the Karnataka High Court's Hijab Judgment, Indian Constitutional Law and Philosophy, <https://indconlawphil.wordpress.com/2022/03/22/guest-post-decisional-autonomy-and-group-privacy-on-the-karnataka-high-courts-hijab-judgment/>

20 Carroll Rainie, S., Kukutai, T., Walter, M., Figueroa-Rodriguez, O. L., Walker, J., & Axelsson, P. (2019). Issues in Open Data - Indigenous Data Sovereignty, The State of Open Data: Histories and Horizons, <https://www.stateofopendata.od4d.net/chapters/issues/indigenous-data.html>

21 See <https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/22018>

this proliferation sufficiently protects individual data and privacy rights, as there is considerable reason to doubt whether formal rights are sufficiently actionable even for individuals in all the circumstances where it matters.

Considering the legal foundations of group and individual data rights		
	Source	Considerations
Individual rights to data protection	Well established through data protection laws	Even the most advanced and progressive data protection laws remain dependent on the awareness and capacity of individuals to exercise their rights, and are not clearly actionable.
Group data rights	International human rights law, select national jurisprudence and subnational law.	Though not yet firmly established as legal rights, there are strong conceptual arguments for the legal foundations of group rights.

Proactive and reactive data governance

We can distinguish between proactive and reactive strategies and interventions for data protection and empowerment. Reactive approaches are those that attempt to address a harm that has been caused or a problem that has emerged. The discourse of data protection is often focused on these types of strategies, for redress or punitive action. Reactive strategies in this vein can involve complaints to authorities or data-using companies, requests for information about data held or data used, or even litigation or administrative procedures to stop data use or actions taken on the basis of data use.

Proactive approaches, on the other hand, are often associated with enabling individuals or groups to exercise better control over their data before it is used or before harms occur. This is sometimes articulated in the context of digital rights literacy and awareness raising. More often, proactive approaches are described in the holistic and ambitious rhetoric of data empowerment or digital self-determination,²² associated with the ways in which data can be leveraged, unblocked, and shared to benefit society, generate economic value, and improve people's lives.

There are obvious conceptual linkages between these two approaches. When people are empowered to better understand how their data is and can be governed, they gain the knowledge that is required to meaningfully claim and enforce their data protection rights. The protection of data from uncontrolled sale and exploitation increases its value and can empower groups to organise and

22 Verhulst, Stefaan G. "Operationalizing digital self-determination." *Data & Policy* 5 (2023)

collectively benefit from the deliberate and informed sharing of that data.

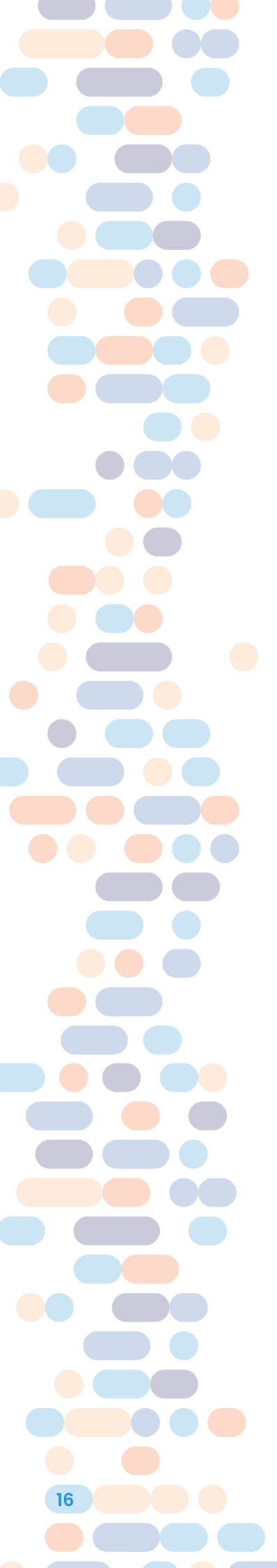
There is nevertheless a tendency for data protection and data empowerment to be viewed as unrelated, or even mutually exclusive phenomena. This is perhaps linked to the very different types of expertise and action required for reactive and proactive strategies for better data governance. While reactive approaches to data protection will often require legal action or expertise for complaints, procedures or litigation, proactive approaches to data empowerment will often involve awareness raising, organisation and mobilisation.

Reactive	Proactive
Addressing harms caused or problems that have emerged.	Enabling individuals or groups to decide in advance how data should be used.
Examples	
Complaints; arbitration; legal action.	Campaigns; institution building; literacy building.

Assessing available actions

Reflecting on some of the distinctions explored above, this section considers what tools and approaches are practically accessible and actionable for individuals and groups that wish to control the collection and use of their data and data that affects them. A preliminary mapping is presented in the below table, distinguishing the tools and approaches that are available to individuals and groups, and between those that are proactive and reactive, as described in the previous section.

Tools and approaches for data governance by individuals and groups		
	Individuals	Groups
Proactive	<p>Individuals can proactively assert control over how their data is collected or used by</p> <ul style="list-style-type: none"> educating themselves about how their data is used by different platforms and services and adapt their online behaviour to avoid specific platforms and services; using privacy-protecting tools like tor browsers, encryption tools, or other technologies; Using data intermediation services to help manage and control their personal data; or declining to share data and use services that would use their data without consent. <p>Notably, these approaches all require awareness and capacity and is much more difficult to apply to data that may impact individuals, but is created or collected by third parties without their knowledge.</p>	<p>Groups such as data collectives and collaboratives can be organised to manage the capacity demands on individuals, and make decisions about services, platforms and sharing on behalf of the group. As with individuals, this is only applicable to data provided 'from' the group. By aggregating individuals' preferences, groups can also strengthen the political power of individuals, which can strengthen their position to negotiate terms of data use, particularly if the group has sole control and access to valuable data.</p>
Reactive	<p>Data protection laws like the GDPR provide individuals with complaint and redress mechanisms with which to take control over how their data is being held and used. Traditional privacy rights might also be asserted in jurisdictions without data protection laws. These legal approaches apply only to personal data as legally defined, and require an individual's awareness, time, and ability to navigate often complex legal processes and corporate policies. When individuals are negatively impacted by data (which may or may not be about them or provided by them) they can also resort to traditional procedures and complaint mechanisms such as those provided by administrative authorities.</p>	<p>Data protection laws often provide no, or limited, rights to bring an action on behalf of a group, limiting the legal route to group redress under data protection legislation. There is, however, a strong precedent for using group rights as a basis for administrative and legal complaints not related to data protection.</p>



Reflecting on the above table highlights that there are relatively few tools and approaches available for either individuals or groups, and the few that do exist are often unevenly accessible in different parts of the world and require significant technical and situational capacities that not everyone has. The tools and approaches available to individuals are much more mature than those available to groups but are far from sufficient. Furthermore, proactive strategies relevant to data ‘from’ or ‘about’ individuals face significant barriers to reaching transformative scale. They may also face significant equity challenges, and by empowering well-resourced groups can risk leaving others behind. At the same time, proactive and reactive group strategies that ignore the existing legal rights of their members may be missing important tools that could bring strength to voluntary cooperation or group actions. Individual data rights, such as the right of an individual to see the data a company holds about them, can be instrumental in revealing systemic problems, but responding to those problems may require group action whether through courts of law, or public mobilisation and the court of public opinion.

The table also reveals a significant gap in actionable tools and strategies to address ‘data that impacts’ both individuals and groups. Data protection law can often be difficult to leverage in these cases, due to strict applicability considerations and challenges in defining the relationship between decision-making and the data on which decisions are based.²³ In such cases, an appeal to substantive rights related to the harm experienced (whether at an individual or group level) might be more effective than asserting data protection rights to challenge problematic, illegitimate or harmful data practices.

It is also worth noting that much of what is referenced above is still evolving or emergent, and there appears to be a complementary development of approaches that can be used for individuals and groups to assert control over their data and the data that affects them. But the toolbox is far from complete, and there are very few truly accessible mechanisms through which people can have a say over their data.

23 For a discussion, see <https://connectedbydata.org/events/2023-09-27-connected-conversation-collective-data-rights>



Aligning and expanding advocacy

Rapid advances in the capacity and implications of aggregated data require that we rethink how data and society interact, and what a fair data future looks like. It has prompted new concerns and focus among the advocacy community, and this is important.

We have also witnessed how discourses around individual and group-based data governance have at times been painted as opposing responses, pulling in opposite directions from the status quo. There may be some for whom concepts of individual data control or collectivisation of data are first-order values, to be prioritised above and to the exclusion of all else. We believe that in the majority of cases, however, individual and group-based approaches are complementary: offering an overlapping set of tools to target and transform the status quo. It is only by having a clearer picture of the particular affordances and limitations of individual and group-based data governance tools, and of the gaps that remain in the data governance toolkit, that we can develop more powerful, inclusive and integrated approaches.

This complementarity can be hard to see, in part because of the ambiguity explored in chapter two. We see this complementarity most clearly when we think about data governance from the perspective of actual people. As considered in chapter three, doing so provides three key insights:

- Individual data protection rights are necessary, but not sufficient, to deliver better governance of data at scale.
- Many group-based data governance approaches are strengthened by building on individual data protections.
- Gaps remain in the data governance toolbox and require interlocking individual and collective governance mechanisms to fill them.

The remainder of this chapter is based on the understanding that there is no fundamental opposition between the premises for individual data protection and group data rights, between proactive strategies and reactive strategies, or between the legal bases of protecting personal and non-personal data. Instead, it takes the complementarity identified above as a starting point for thinking about how to better advocate for better data governance. This is an opportunity for the advocacy community to coordinate and amplify our common efforts towards fixing the status quo, rather than pull in opposite directions and dilute our efforts.



Recommendations for more impactful advocacy

Based on our analysis and organisational dialogue, we draw five high-level recommendations for advocates in the data space:

#1 Use the language of “personal data” with caution.

Debates about whether data is personal data or non-personal data can be misleading, inadvertently excluding data “about me” and data “that impacts me” from the scope of political discussion. Advocates should beware of categorical distinctions between personal and non-personal data in legislation and corporate policy, and take care not to reinforce arbitrary distinctions that disempower people and their control over the data that affects them.

#2 Be wary of simple solutions.

The ambiguities explored in section two can encourage simplified thinking about data governance. While simple messaging and communication are often powerful, carefully considering the distinctions proposed in that section can help refine the strategies and communication that underpin effective advocacy. We should be mindful of how the right mix of complementary strategies focused on groups and individuals can help us achieve our near-term goals. We also need to remain attuned to the very limited scope of tools and approaches available for people to control their data, and recognize that the fair data future we aim to facilitate will inevitably require a coherent combination of individual and group rights and protections. We need to start laying a nuanced foundation for this now.

#3 Balance legal advocacy with other approaches.

The proliferation of data protection laws is an important milestone, and further work needs to be done to establish and expand the legally actionable rights of individuals and groups to control how their data is used. Even when strong legal rights and protections are established, however, they can often be difficult to invoke or implement, and the principles they represent will rarely be immediately implemented in practice by companies and government agencies. Action-focused advocacy can support legal advances in many ways. Collective action campaigns can help to activate legal protections or remedies. Legal awareness raising and capacity development can raise the expectations and capacities of the general public, and incentivize decision-makers towards reform. In this sense, the law is both an important and multi-functional tool in the advocacy toolbox. It is likely to be most effectively leveraged in context and combination with other advocacy strategies. Multi-functional teams with lawyers and other types of experts can be especially well suited to this kind of advocacy.



#4 Coordinate meaningfully and visibly.

We are more than the sum of our parts, and we need to embrace the complementarity of our various focus areas and expertise to pursue the complex systems change we aspire to. For advocacy initiatives aligned with a particular pole on the continuum between “personal data” and “collective governance” this is an imperative and an opportunity to coordinate our efforts. We should align our strategies and our messaging to be mutually supportive of the futures we are working towards. We should do so in ways that maintain our distinct contributions to the advocacy ecosystem in which we operate, but that recognize and broadcast how the puzzle pieces fit together. Collaborative communications, projects, and fundraising can help signal to the wider community of stakeholders the importance of thinking holistically about individuals, groups, and data governance.

#5 Remember that narratives matter.

At the end of the day, successful advocacy often depends on having a good story, about why the issue matters, about how the outcome will affect us and others, about why people should care in the first place. These stories are inevitably informed by subtle but widely recognised narratives about data and society, and most of those narratives have been established by powerful stakeholders like governments and companies. They often rely on some of the ambiguities explored in section two to limit the scope of people to take control of their data and the way it is used to impact their lives. In the wake of increasing public awareness about data privacy and AI, the advocacy community has an opportunity to craft new narratives that move beyond implicit dichotomies about personal or non-personal data, about individuals or groups. We have an opportunity to build new narratives about people, control, and a fair data future. This is the story we should tell when we communicate, litigate, train and explore. We’re all in this together.



About the organisations

MyData Global's mission is to empower individuals by improving their right to self-determination regarding their personal data.

Apti Institute works for an equitable and just digital world where people are empowered to negotiate with technology.

The Datasphere Initiative is dedicated to global collaboration on technical and policy solutions for the urgent, multidimensional, and cross-border challenges of data governance.

Connected by Data campaigns to put community at the centre of data narratives, practices and policies by advocating for collective and open data governance.

About this publication

Authors: Christopher Wilson (MyData Global), Tim Davies (Connected by Data), Vinay Narayan and Avani Airan (Apti Institute), Viivi Lähteenoja (MyData Global), Carolina Rossini and Sophie Tomlinson (The Datasphere Initiative)

Design: Silke Sepp

Citation information: Wilson, C., Davies, T., Narayan, V., Airan, A., Lähteenoja V., Rossini, C., and Tomlinson, S. (2023) In this together: Combining individual and collective strategies to confront data power.

Published December 1, 2023.

This paper may be shared or adapted with attribution under Creative Commons Attribution 4.0 International (CC BY 4.0).

Download this publication at <https://mydata.org/publications>