UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

Rethinking data and rebalancing digital power

Pavel, V.; Rethinking data working group

Publication date
2022
Document Version
Final published version
License
CC BY

Link to publication

Citation for published version (APA):
Pavel, V., & Rethinking data working group (2022). *Rethinking data and rebalancing digital power*. Ada Lovelace Institute. https://www.adalovelaceinstitute.org/project/rethinking-data/

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)

Download date:05 Sept 2026

Ada Lovelace Institute

Rethinking data and rebalancing digital power

Design: Eureka! Illustration: Shout

Contents

Letter from the working group co-chairs 4

A call for a new vision 7

How to use this report 11

Chapter 1:
Understanding power in data-intensive digital ecosystems 13

1. Context setting 14
2. Rethinking regulatory approaches in digital markets 17
3. Weak enforcement response in digital markets 22

Chapter 2:
Making data work for people and society 27

1. Transforming infrastructure through open ecosystems 29
2. Reclaiming control of data from dominant companies 45
3. Rebalancing the centres of digital power with new (non-commercial) institutions 57
4. Ensuring public participation in technology policy making 71

Chapter 3:
Conclusions and open questions 79

1. Effective regulatory enforcement 81
2. Legal action and representation 83
3. Removing industry dependencies 84

Open invitation and call to action 87

Final notes 90

Letter from the working group co-chairs

This project by an international and interdisciplinary working group of experts from academia, policy, law, technology and civil society, invited by the Ada Lovelace Institute, had a big ambition: to imagine rules and institutions that can shift power over data and make it benefit people and society.

We began this work in 2020, only a few months into the pandemic, at a time when public discourse was immersed in discussions about how technologies – like contact tracing apps – could be harnessed to help address this urgent and unprecedented global health crisis.

The potential power of data to affect positive change – to underpin public health policy, to support isolation, to assess infection risk – was perhaps more immediate than at any other time in our lives. At the same time, concerns such as data injustice and privacy remained.

It was in this climate that our working group sought to explore the relationship people have with data and technology, and to look towards a positive future that would centre governance, regulation and use of data on the needs of people and society, and contest the increasingly entrenched systems of digital power.

The working group discussions centred on questions about power over both data infrastructures, and over data itself. Where does power reside in the digital ecosystem, and what are the sources of this power? What are the most promising approaches and interventions that might distribute power more widely, and what might that rebalancing accomplish?

The group considered interventions ranging from developing public-service infrastructure to alternative business models, from fiduciary duties for data infrastructures to a new regime for data under a public-interest approach. Many were conceptually interesting but required more detailed thought to be put into practice.

Through a process of analysis and distillation, that broad landscape narrowed to four areas for change: infrastructure, governance, institutions and democratic participation in decisions over data processing, collection and use. We are happy that the group has endorsed a pathway towards transformation, identifying a shared vision and practical interventions to begin the work of changing the digital ecosystem.

Throughout this process, we wanted to free ourselves from the constraints of currently perceived models and norms, and go beyond existing debates around data policy. We did this intentionally, to extend the scope of what is politically thought to be possible, and to create space for big ideas to flourish and be discussed.

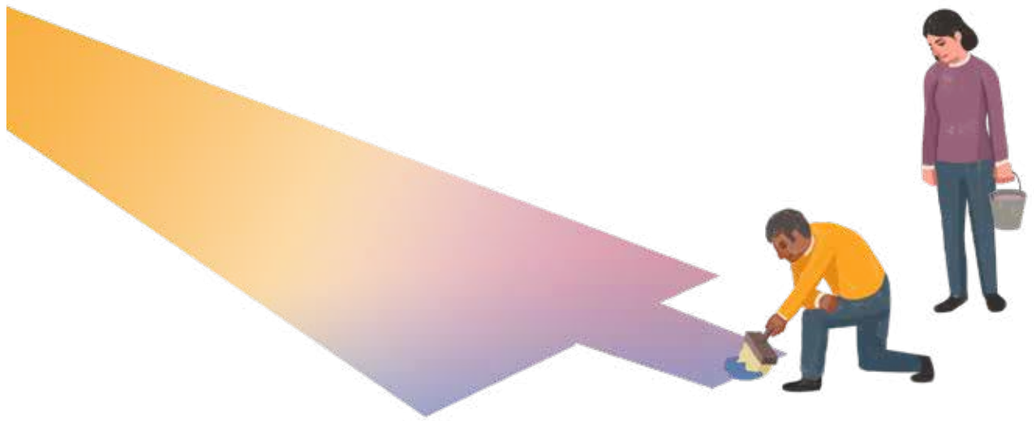
We see this work as part of one of the most challenging efforts we have to make as humans and as societies. Its ambitious aim is to bring to the table a richer set of possibilities of our digital future. We uphold that we need new imaginaries if we are to create a world where digital power is distributed among many and serves the public good, as defined in democracies.

We hope this report will serve as both a provocation and a way to generate constructive criticism and mature ideas on how to transform digital ecosystems, but also a call to action for those of you – our readers – who hold the power to make the interventions we describe into political and business realities.

Diane Coyle
Bennett Professor of Public Policy, University of Cambridge

Paul Nemitz
Principal Adviser on Justice Policy, European Commission and visiting Professor of Law at College of Europe

Co-chairs
Rethinking data working group



A call for a new vision

In 2020, the Ada Lovelace Institute characterised the digital ecosystem as:

- **Exploitative:** Data practices are exploitative, and they fail to produce the potential social value of data, protect individual rights and serve communities.

- **Shortsighted:** Political and administrative institutions have struggled to govern data in a way that enables effective enforcement and acknowledges its central role in the data-driven systems.

- **Disempowering:** Individuals lack agency over how their data is generated and used, and there are stark power imbalances between people, corporations and states.[1]

We recognised an urgent need for a comprehensive and transformative vision for data that can serve as a 'North Star', directing our efforts and encouraging us to think bigger and move further.

Our work to 'rethink data' began with a forward-looking question: 'What is a more ambitious vision for data use and regulation that can deliver a positive shift in the digital ecosystem towards people and society?'

This drove the establishment of an expert working group (see 'Acknowledgements', page 92), bringing together leading thinkers in privacy and data protection, public policy, law and economics from the technology sector, policy, academia and civil society across the UK, Europe, USA, Canada and Hong Kong.

This disciplinarily diverse group brought their perspectives and expertise to understand the current data ecosystem and make sense of the complexity that characterises data governance in the UK, across Europe and internationally. Their reflection on the challenges informed a holistic approach to the changes needed, which is highly relevant to the jurisdictions mentioned above, and which we hope will be of foundational interest to related work in other territories.

Understanding that shortsightedness limits creative thinking, we deliberately set the field of vision to the medium term, 2030 and beyond. We intended to escape the 'policy weeds' of unfolding developments in data and technology policy in the UK, EU or USA, and set our sights on the next generation of institutions, governance, infrastructure and regulations.

Using discussions, debates, commissioned pieces, futures-thinking workshops, speculative scenario building and horizon scanning, we have distilled a multitude of ideas, propositions and models. (For full details about our methodology, see 'Final notes' on page 90.)

These processes and methods moved the scope of enquiry on from the original premise – to articulate a positive ambition for the use and regulation of data that recognised asymmetries of power and enabled social value – to seeking the most promising interventions that address the significant power imbalances that exist between large private platforms, and groups of people and individuals.

This report highlights and contextualises four cross-cutting interventions with a strong potential to reshape the digital ecosystem:

1. Transforming infrastructure into open and interoperable ecosystems.
2. Reclaiming control of data from dominant companies.
3. Rebalancing the centres of power with new (non-commercial) institutions.
4. Ensuring public participation as an essential component of technology policymaking.

The interventions are multidisciplinary and they integrate legal, technological, market and governance solutions. They offer a path towards addressing present digital challenges and the possibility for a new, healthy digital ecosystem to emerge.

What do we mean by a healthy digital ecosystem? One that privileges people over profit, communities over corporations, society over shareholders. And, most importantly, one where power is not held by a few large corporations, but is distributed among different and diverse models, alongside people who are represented in, and affected by the data used by those new models. The digital ecosystem we propose is balanced, accountable and sustainable, and imagines new types of infrastructure, new institutions and new governance models that can make data work for people and society.

Some of these interventions can be located within (or built from) emerging and recently adopted policy initiatives, while others require the wholesale overhaul of regulatory regimes and markets. They are designed to spark ideas that political thinkers, forward-looking policymakers, researchers, civil society organisations, funders and ethical innovators in the private sector consider and respond to when designing future regulations, policies or initiatives around data use and governance.

This report also acknowledges the need to prepare the ground for the more ambitious transformation of power relations in the digital ecosystem. Even a well-targeted intervention won't change the system unless it is supported by relevant institutions and behavioural change.

In addition to targeted interventions, the report explains the preconditions that can support change:

1. Effective regulatory enforcement.
2. Legal action and representation.
3. Removal of industry dependencies.

Reconceptualising the digital ecosystem will require sustained, collective and thorough efforts, and an understanding that elaborating on strategies for the future involves constant experimentation, adaptation and recalibration.

Through discussion of each intervention, the report brings an initial set of provocative ideas and concepts, to inspire a thoughtful debate about the transformative changes needed for the digital ecosystem to start evolving towards a people and society-focused vision. These can help us think about potential ways forward, open up questions for debate instead of rushing to provide answers, and offer a starting point from which more fully fledged solutions for change are able to grow.

We hope that policymakers, researchers, civil society organisations, funders and ethical industry innovators will engage with – and, crucially, iterate on – these propositions in a collective effort to find solutions that lead to lasting change in data practices and policies.

What do we mean by a healthy digital ecosystem? One that privileges people over profit, communities over corporations, society over shareholders. And, most importantly, one where power is not held by a few large corporations, but is distributed among different and diverse models, alongside people who are represented in, and affected by the data used by those new models.

Making data work for people and society

The building blocks for a people-first digital ecosystem start from **repurposing data** to respect individual agency and deliver societal benefits, and from **addressing abuses** that are well defined and understood today, and are likely to continue if they are not dealt with in a systemic way.

Making data work for people means protecting individuals and society from abuses caused by corporations' or governments' use of data and algorithms. This means fundamental rights such as privacy, data protection and non-discrimination are both protected in law and reflected in the design of computational processes that generate and capture personal data.

The requirement to protect people from harm does not only operate in the present, there is also a need to **prevent** harms from happening in the future, and to create resilient institutions that will operate effectively against future threats and potential impact that can't be fully anticipated.

To produce long-lasting change, we will need to **break structural dependencies** and address **the sources of power** of big technology companies. To do this, one goal must be to create data governance models and new institutions that will balance power asymmetries. Another goal is to restructure economic, technical and legal tools and incentives, to move infrastructure control away from unaccountable organisations.

Finally, **positive goals for society** can emerge from data infrastructures and algorithmic models developed by private and/or public actors, if data serves both individual and societal goals, rather than just the interests of commerce or undemocratic regimes.

How to use this report

The report is written to be of particular use to policymakers, researchers, civil society organisations, funders and those working in data-governance. To understand how and where you can take the ideas explored here forward, we recommend these approaches:

- If you work on **data policy decision-making**, go through a brief overview of the sources of power in today's digital ecosystem in Chapter 1, focus on 'The vision' subsections in Chapter 2 and answer the call to action in Chapter 3 by considering ways to translate the proposed interventions into policy action and help build the pathway towards a comprehensive and transformative vision for data.

- If you are a **researcher**, focus on the 'How to get from here to there' and 'Further considerations and provocative concepts' subsections in Chapter 2 and answer the call to action in Chapter 3 by reflecting critically on the provocative concepts and help develop the propositions into more concrete solutions for change.

- If you are a **civil society organisation**, focus on 'How to get from here to there' subsections in Chapter 2 and answer the call to action in Chapter 3 by engaging with the suggested transformations and build momentum to help visualise a positive future for data and society.

- If you are a **funder**, go through an overview of the sources of power in today's digital ecosystem in Chapter 1, focus on 'The vision' subsections in Chapter 2 and answer the Call to action in Chapter 3 by supporting the development of a proactive policy agenda by civil society.

- If you are working on **data governance in industry**, focus on sections 1 and 2 in Chapter 2, help design mechanisms for responsible generation and use of data, and answer the call to action in Chapter 3 by supporting the development of standards for open and rights enhancing systems.

Understanding power in data-intensive digital ecosystems

1. Context setting

To understand why a transformation is needed in the way our digital ecosystem operates, it's necessary to understand the dynamics and different facets of today's data-intensive ecosystem.

In the last decade, there has been an exponential increase in the generation, collection and use of data. This upsurge is driven by an increasing datafication of everyday parts of our lives,[2] from work to social interactions and, to the provision of public services. The backbone of this change is the growth of digitally connected devices, data infrastructures and platforms, which enable new forms of data generation and extraction at an unprecedented scale.

Estimates put the volume of data created and consumed from two zettabytes in 2010 to 64.2 zettabytes in 2020 (one zettabyte is a trillion gigabytes) and project that it will grow to more than 180 zettabytes up to 2025.[3] These oft-cited figures disguise a range of further dynamics (such as the wider societal phenomena of discrimination and inequality that are captured and represented in these datasets), and the textured landscape of who and what is included in the datasets, what data quality means in practice, and whose objectives are represented in data processes and met through outcomes from data use.

Data is often promised to be transformative, but there remains debate as to exactly what it transforms. On one hand, data is recognised as an important economic opportunity, and policy focus across the globe and is believed to deliver significant societal benefits. On the other hand, increased datification and calculability of human interactions can lead to human rights abuses and illegitimate public or private control. In between these opposing views are a variety of observations that reflect the myriad ways data and society interact, broadly considering the ways such practices reconfigure activities, structures and relationships.[4]

> It it is hard to understand power from data without understanding complex technological interactions up and down the whole technology 'stack', from the basic protocols and connectivity that underpin technologies, through hardware, and the software and cloud services that are built on them.

According to scholars of surveillance and informational capitalism, today's digital economy is built on deeply rooted, exploitative and extractive data practices.[5] These result in the accrual of immense surpluses of value to dominant technology corporations, and a role for the human participants enlisted in value creation for these big technology companies that has been described as a form of 'data rentiership'.[6]

Commentators differ, however, on the real source of the value that is being extracted. Some consider that value comes from data's predictive potential, while others emphasise that the economic arrangements in the data economy allow for huge profits to be made (largely through the advertising-based business model) even if predictions are much less effective than technology giants claim.[7]

In practice, only a few large technology corporations – Alphabet (Google), Amazon, Apple, Meta Platforms (Facebook) and Microsoft – have the data, processing abilities, engineering capacity, financial resources, user base and convenience appeal to provide a range of services that are both necessary to smaller players and desired by a wide base of individual users.

These corporations extract value from their large volumes of interactions and transactions, and process massive amounts of personal and non-personal data in order to optimise the service and experience of each business or individual user. Some platforms have the ability to simultaneously coordinate and orchestrate multiple sensors or computers in the network, like smartphones or connected objects. This drives the platform's ability to innovate and offer services that seem either indispensable or unrivalled.

While there is still substantial innovation outside these closed ecosystems, the financial power of the platforms means that in practice they are able to either acquire or imitate (and further improve) innovations in the digital economy. Their efficiency in using this capacity enables them to leverage their dominance into new markets. The acquisition of open-source code platforms like GitHub by Microsoft in 2018 and RedHat by IBM in 2019 also points to a possibility that incumbents intend to extend their dominance to open-source software. The difficulty new players face to compete makes the largest technological players seem unmovable and unchangeable.

Over time, access to large pools of personal data has allowed platforms to develop services that now represent and influence the infrastructure or underlying basis for many public and private services. Creating ever-more dependencies in both public and private spheres, large technology companies are extending their services to societally sensitive areas such as education and health.

This influence has become more obvious during the COVID-19 pandemic, when large companies formed contested public-private partnerships with public health authorities.[8] They also partnered among themselves to influence contact tracing in the pandemic response, by facilitating contact tracing technologies in ways that were favourable or unfavourable to particular nation states. This revealed the difficulty, even at state level, of engaging in advanced use of data without the cooperation of the corporations that control the software and hardware infrastructure.

Focusing on data alone is insufficient to understand power in data-intensive digital systems. A vast number of interrelated factors consolidate both economic and societal power of particular digital platforms.[9] These factors go beyond market power and consumer behaviour, and extend to societal and democratic influence (for example through algorithmic curation and controlling how human rights can be exercised).[10]

Theorists of platform governance highlight the complex ways in which vertically integrated platforms make users interacting with them legible to computers, and extract value by intermediating access to them.[11] This makes it hard to understand power from data without understanding complex technological interactions up and down the whole technology 'stack', from the basic protocols and connectivity that underpin technologies, through hardware, and the software and cloud services that are built on them.[12]

Large platforms have become – as a result of laissez-faire policies (minimal government intervention in market and economic affairs) rather than by deliberate, democratic design – one of the building blocks for data governance in the real world, unilaterally defining the user experience and consumer rights. They have used a mix of law, technology and economic influence to place themselves in a position of power over users, governments, legislators and private-sector developers, and this has proved difficult to dislodge or alter.[13]

2. Rethinking regulatory approaches in digital markets

There is a recent, growing appetite to regulate both data and platforms using a variety of legal approaches to regulate market concentration, platforms as public spheres, and data and AI governance. The year 2021 alone marked a significant global uptick in proposals for the regulation of AI technologies, online markets, social media platforms and other digital technologies, with more still to come in 2022.[14]

A range of jurisdictions are reconsidering the regulation of digital platforms both as marketplaces and places of public speech and opinion building ('public spheres'). Liability obligations are being reanalysed, including in bills around 'online harms' and content moderation. The Online Safety Act in Australia,[15] India's Information Technology Rules,[16] the EU's Digital Services Act[17] and the UK's draft Online Safety Bill[18] are all pieces of legislation that seek to regulate more rigorously the content and practices of online social media and messaging platforms.

Steps are also being made to rethink the relationship between competition, data and platforms, and jurisdictions are using different approaches. In the UK, the Competition and Markets Authority launched the Digital Markets Unit, focusing on a more flexible approach, with targeted interventions in competition in digital markets and codes of conduct.[19] In the EU, the Digital Markets Act (DMA) takes a top-down approach and establishes general rules for large companies that prohibit certain practices up front, such as combining or cross-using personal data across services without users' consent, or giving preference to their own services and products in rankings.[20] India is also responding to domestic market capture and increased influence from large technology companies with initiatives such as the Open Network for Digital Commerce, which aims to create a decentralised and interoperable platform for direct exchange between buyers and sellers without intermediary services such as Amazon.[21] At the same time, while the draft 2019 Indian Data Protection Bill is being withdrawn, a more comprehensive legal framework is expected in 2022 covering – alongside privacy and data protection – broader issues such as non-personal data, regulation of hardware and devices, data localisation requirements and rules to seek approval for international data transfers.[22]

Developments in data and AI policy

Around 145 countries now have some form of data privacy law, and many new additions or revisions are heavily influenced by legislative standards including the Council of Europe's Convention 108 + and the EU General Data Protection Regulation (GDPR).[23]

The GDPR is a prime example of legislation aimed at curbing the worst excesses of exploitative data practices, and many of its foundational elements are still being developed and tested in the real world. Lessons learned from the GDPR show how vital it is to consider power within attempts to create more responsible data practices. This is because regulation is not just the result of legal design in isolation, but is also shaped by immense corporate lobbying,[24] applied within organisations via their internal culture and enforced in a legal environment that gives major corporations tools to stall or create disincentives to enforcement.

In the United States, there have been multiple attempts at proposing privacy legislation,[25] and there is growing momentum with privacy laws being adopted at the state level.[26] A recent bipartisan privacy bill proposed in June 2022[27] includes broad privacy provisions, with a focus on data minimisation, privacy by design and by default, loyalty duties to individuals and the introduction of a private right to action against companies. So far, the US regulatory approach to new market dynamics has been a suite of consumer protection, antitrust and privacy laws enforced under the umbrella of a single body, the Federal Trade Commission (FTC), which has a broad range of powers to protect consumers and investigate unethical business practices.[28]

Since the 1990s, with very few exceptions, the US technology and digital markets have been dominated by a minimal approach to antitrust intervention[29] (which is designed to promote competition and increase consumer welfare). Only recently has there been a revival of antitrust interventions in the US with a report on competition in the digital economy[30] and cases launched against Facebook and Google.[31]

In the UK, a consultation launched in September 2021 proposed a number of routes to reform the Data Protection Act and the UK GDPR.[32] Political motivations to create a 'post-Brexit' approach to data protection may test 'equivalence' with the European Union, to the detriment of the benefits of coherence and seamless convergence of data rights and practices across borders.

There is also the risk that the UK lowers levels of data protection to try to increase investment, including by large technology companies operating in the UK, therefore reinforcing their market power. Recently released policy documents containing significant changes are the National Data and AI Strategies,[33] and the Government's response to the consultation on the reforms to the data protection framework,[34] followed by a draft bill published in July 2022.[35]

Joining the countries that have developed AI policies and national strategies,[36] Brazil,[37] the USA[38] and the UK[39] launched their own initiatives, with regulatory intentions ranging from developing ethical principles and guidelines for responsible use, to boosting research and innovation, to becoming a world leader, an 'AI superpower' and a global data hub. Many of these initiatives are industrial policy rather than regulatory frameworks, and focus on creating an enabling environment for the rapid development of AI markets, rather than mitigating risk and harms.[40]

In August 2021, China adopted its comprehensive data protection framework consisting of the Personal Information Protection Law,[41] which is modelled on the GDPR, and the Data Security Law, which focuses on harm to national security and public interest from data-driven technologies.[42] Researchers argue that understanding this unique regulatory approach should not start from a comparative analysis (for example to jurisdictions such as the EU, which focus on fundamental rights). They trace its roots to the Chinese understanding of cybersecurity, which aims to protect national polity, economy and society from data-enabled harms and defend against vulnerabilities.[43]

While some of these recent initiatives have the potential to transform market dynamics towards less centralised and less exploitative practices, none of them meaningfully contest the dominant business model of online platforms or promote ethical alternatives. Legislators seem to choose to regulate through large actors as intermediaries, rather than by reimagining how regulation could support a more equal distribution of power. In particular, attention must be paid to the way many proposed solutions tacitly require 'Big Tech' to stay big.[44]

The EU's approach to platform, data and AI regulation

In the EU, the Digital Services Act (DSA) and the Digital Markets Act (DMA) bring a proactive approach to platform regulation, by prohibiting certain practices up front and introducing a comprehensive package of obligations for online platforms.

The DSA sets clear obligations for online platforms against illegal content and disinformation and prohibits some of the most harmful practices used by online platforms (such as using manipulative design techniques and targeted advertising based on exploiting sensitive data).

It mandates increased transparency and accountability for key platform services (such as providing the main parameters used by recommendation systems) and includes an obligation for large companies to perform systemic risk assessments. This is complemented with a mechanism for independent auditors and researchers to access the data underpinning the company's risk assessment conclusions and scrutinise the companies' mitigation decisions.

While this is undoubtedly a positive shift, the impact of this legislation will depend substantially on online platforms' readiness to comply with legal obligations, their interpretation of new legal requirements and effective enforcement (which has proved challenging in the past, for example with the GDPR).

The DMA addresses anticompetitive behaviour and unfair market practices of platforms that – according to this legislation – qualify as 'gatekeepers'. Next to a number of prohibitions (such as combining or cross-using personal data without user consent), which are aimed at preventing the gatekeepers' exploitative behaviour, the DMA contains obligations that – if enforced properly – will lead to more user choice and competition in the market for digital services.

These include basic interoperability requirements for instant messaging services, as well as interoperability with the gatekeepers' operating system, hardware and software when the gatekeeper is providing complementary or supporting services.[45] Another is the right for business users of the gatekeepers' services to obtain free-of-charge, high quality, continuous and real-time access to data (including personal data) provided or generated in connection with their use of the gatekeepers' core service.[46] End users will also have the right to exercise the portability of their data, both provided as well as generated through their activity on core services such as marketplaces, app stores, search and social media.[47]

The DMA and DSA do not go far enough in terms of addressing deeply rooted challenges, such as supporting alternative business models that are not premised on data exploitation or speaking to users' expectations to be able to control algorithmic interfaces (such as the interface for content filtering/ generating recommendations). Nor does it create a level playing field for new market players who would like to develop services that compete with the gatekeepers' core services.

New approaches to data access and sharing are also seen with the adopted Data Governance Act (DGA)[48] and the draft Data Act.[49] The DGA introduces the concept of 'data altruism' (the possibility for individuals or companies to voluntarily share data for the public good), facilitates the re-use of data from public and private bodies, and creates rules for data intermediaries (providers of data sharing services that are free of conflicts of interests relating to the data they share).

Complementing this approach, the proposed Data Act aims at securing end users' right to obtain all data (personal, non-personal, observed or provided) generated by their use of products such as wearable devices and related services. It also aims to develop a framework for interoperability and portability of data between cloud services, including requirements and technical standards enabling common European data spaces.

There is also an increased focus on regulating the design and use of data-driven technologies, such as those that use artificial intelligence (machine learning algorithms). The draft Artificial Intelligence Act (AI Act) follows a risk-based approach that is limited to regulating 'unacceptable' and high-risk AI systems, such as prohibiting AI uses that pose a risk to fundamental rights or imposing ex ante design obligations on providers of high-risk AI systems.[50]

Perhaps surprisingly, the AI Act, as proposed by the European Commission, does not impose any transparency or accountability requirements on systems that pose less than high risk (with the exception of AI system that may deceive or confuse consumers), which include the dominant commercial business-to-consumer (B2C) services (e.g. search engines, social media, some recommendation systems, health monitoring apps, insurance and payment services).

Regardless of the type of risk (high-risk or limited-risk), this approach leaves a significant gap in accountability requirements for both large and small players that could be responsible for creating unfair AI systems. Responsibility measures should aim both at regulating the infrastructural power of large technology companies that supply most of the tools for 'building AI' (such as large language models, cloud computing power, text and speech generation and translation), as well as at creating responsibility requirements for smaller downstream providers who make use of these tools to construct their underlying services.

3. Weak enforcement response in digital markets

Large platforms are by their nature multi-sided, multi-sectoral and operate globally. The regulation of their commercial practices cuts across many sectors, and they are overseen by multiple bodies in different jurisdictions with varying degrees of expertise and in-house knowledge about how platforms operate. These include consumer protection authorities, data protection and competition authorities, non-discrimination and equal opportunities bodies, and financial markets, telecom regulators, media regulators, etc.).

It is well known that these regulatory bodies are frequently under-equipped for the task they are charged with, and there is an asymmetry between the resources available to them compared to the resources large corporations invest in neutralising enforcement efforts. For example, in the EU there is an acute lack of resources and institutional capacity: half the data protection authorities in the EU have an annual budget of €5 million or less, and 21 of the data protection authorities declare that their existing resources are not enough to operate effectively.[51]

But a bigger problem is the lack of regulatory response in general, and recent lessons learned from insufficient data-protection enforcement responses show there needs to be a shift towards a stronger response from regulators, and a more proactive, collaborative approach to curbing exploitative and harmful activities, and bringing down illegal practices.

For example, in 2018 the first complaints against the invasive practices of the online advertising industry (such as real-time bidding, an online ad auctioning system that broadcasts personal data to thousands of companies)[52] were filed with the Irish Data Protection Commissioner (Irish DPC) and with the UK's Information Commissioner Office (ICO),[53] two of the more resourceful – but still not sufficiently funded – authorities. Similar complaints followed across the EU.

> There needs to be a stronger response from regulators, and a more proactive, collaborative approach to curbing exploitative and harmful activities.

After three years of inaction, civil society groups initiated court cases against the two regulators for lack of enforcement, as well as a lawsuit against major advertising and tracking companies.[54] It was a relatively small regulator, the Belgian Data Protection Authority, that confirmed in its 2022 decision that those ad tech practices are illegal, showing that the lack of resources is not the sole cause for regulatory inertia.[55]

Some EU data protection authorities have been criticised for their reluctance to intervene in the technology sector. For example, it took three years from launching the investigation for the Irish regulator to issue a relatively small fine against WhatsApp for failure to meet transparency requirements under the GDPR.[56] The authority is perceived as a key 'bottleneck' to enforcement because of its delays in delivering enforcement decisions,[57] as many of the large US technology companies are established in Dublin.[58]

Some have suggested that 'reform to centralise enforcement of the GDPR could help rein in powerful technology companies'.[59] The Digital Markets Act (DMA) awards the European Commission the role of a sole enforcer against certain data-related practices performed by 'gatekeeper' companies (for example the prohibition of combining and cross-using personal data from different services without consent). The enforcement mechanism of the DMA gives powers to the European Commission to target selected data practices that may also infringe rules typically governed by the GDPR.

In the UK, the ICO has been subject to criticism for its preference for dialogue with stakeholders over formal enforcement of the law. Members of Parliament as well as civil society organisations have increasingly voiced their disquiet over this approach,[60] while academics have queried how the ICO might be held accountable for its selective and discretionary application of the law.[61]

The 2021 public consultation led by the UK Government – *Data: A New Direction* – will do little to reassure those concerned, given the significant incursions into the ICO's regulatory independence mooted.[62] It remains to be seen whether subsequent consultations initiated by the ICO regarding its regulatory approach signal a shift from selective and discretionary application of law towards formal enforcement action.[63]

The measures proposed for consultation go even further towards removing some of the important requirements and guardrails against data abuses, which in effect will legitimise practices that have been declared illegal in the EU.[64]

Recognising the need for cooperation among different regulators

Examinations of abuses, market failure, concentration tendencies in the digital economy and market power of large platforms are more prominent. Extensive reports were commissioned by governments in the UK,[65] Germany,[66] the European Union,[67] Australia[68] and beyond, asking what transformations are necessary in competition policy, to address the challenges of the digital economy.

A comparison of these four reports highlights the problem of under-enforcement in competition policy and recommends a more active enforcement response.[69] It also underlines that all the reports analyse the important interplay between competition policy and other policies such as data protection and consumer protection law.

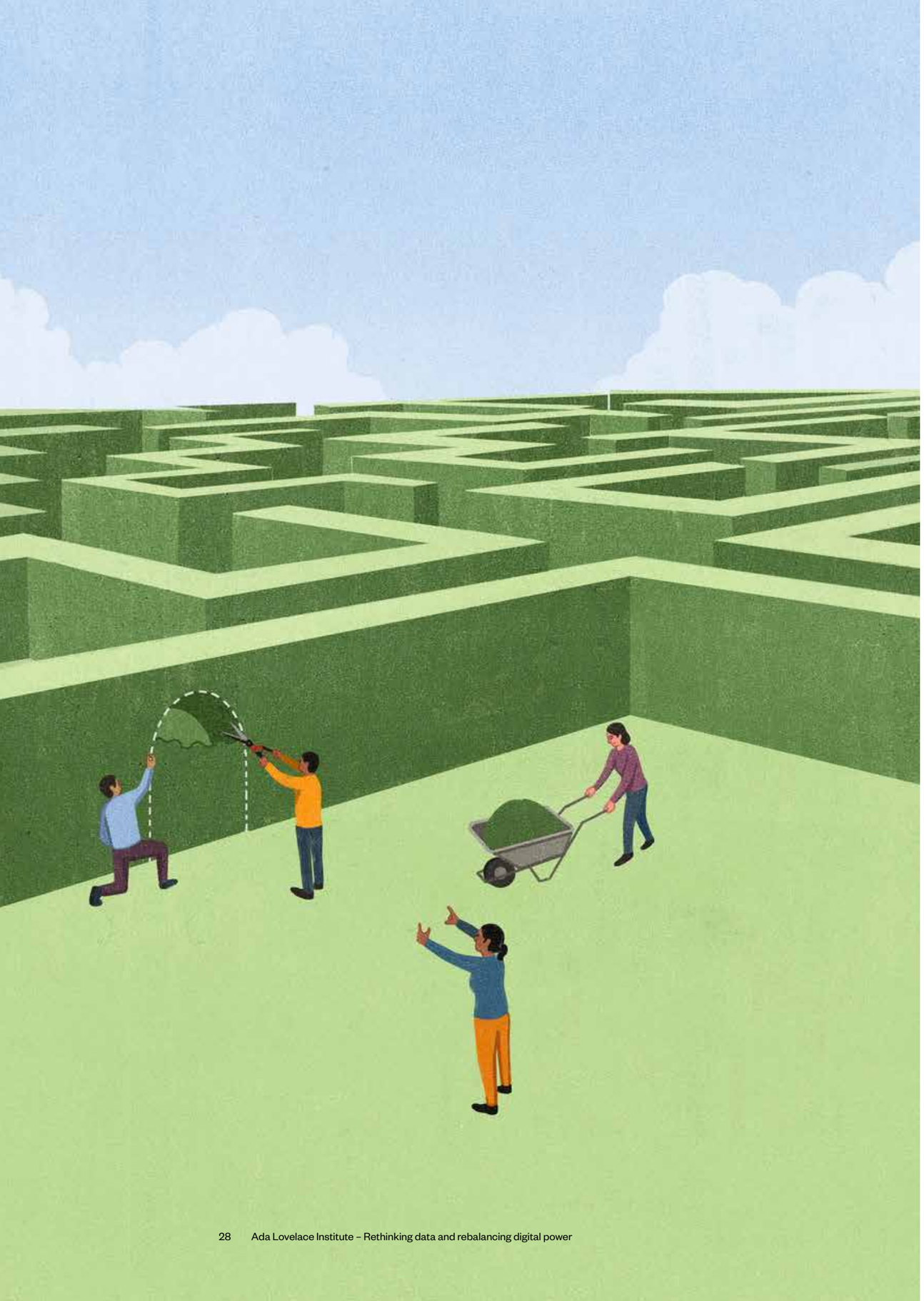
The Furman report in the UK recommended the creation of a new Digital Markets Unit that collaborates on enforcement with regulators in different sectors and draws on their experience to form a more robust approach to regulating digital markets.[70] In 2020, the UK Digital Regulation Cooperation Forum (DRCF) was established to enhance cooperation between the Competition and Markets Authority (CMA), the Information Commissioner's Office (ICO), the Office of Communications (Ofcom) and the Financial Conduct Authority (FCA) and support a more coordinated regulatory approach.[71]

The need for more collaboration and joined-up thinking among regulators was highlighted by the European Data Protection Supervisor (EDPS) in 2014.[72] In 2016, the EDPS launched the Digital Clearinghouse initiative, an international voluntary network of enforcement bodies in different fields,[73] however its activity has been limited.

Today there is still limited collaboration between regulators across sectors and borders because of a lack of legal basis for effective cooperation and exchange of information, including compelled and confidential information. Support for a more proactive and coherent regulatory enforcement must increase substantially to make a significant impact in terms of limiting the overwhelming power of large technology corporations in markets, over people and in democracy.

Chapter 2

Making data work for people and society



This chapter explores four cross-cutting interventions that have the potential to shift power in the digital ecosystem, especially if implemented in coordination with each other. These provocative ideas are offered with the aim to push forward the thinking around existing data policy and practice.

Each intervention is capable of integrating legal, technological, market and governance solutions that could help transition the digital ecosystem towards a people-first vision. While there are many potential approaches, for the purposes of this report – for clarity and ease of understanding –one type of potential solution or remedy is focused on under each intervention.

Each intervention is woven and connected to the others in a way that sets out a cross-cutting vision of an alternative data future, and which can frame forward-looking debates about data policy and practice. The vision these interventions offer will require social and political standing. Behind each intervention there is a promise of a positive change that needs the support and collaboration of policymakers, researchers, civil society organisations and industry practitioners to make them into a reality.

1. Transforming infrastructure through open ecosystems

The vision

Imagine a world in which digital systems have been transformed, and control over technology infrastructure and algorithms no longer lies in the hands of a few large corporations.

Transforming infrastructure means what was once a closed system of structural dependencies, which enabled large corporations to concentrate power, has been replaced by an open ecosystem where power imbalances are reduced and people can shape the digital experiences they want.

No single company or subset of companies controls the full technological stack of digital infrastructures and services. Users can exert meaningful control over the ways an operating system functions on phones and computers, and actions performed by web browsers and apps.

The incentive structures that drove technology companies to entrench power have been dismantled, and new business models are more clearly aligned with user interests and societal benefits. This means there are no more 'lock in' models, in which users find it burdensome to switch to another digital service provider, and fewer algorithmic systems that are optimised to attract clicks, prioritising advertising revenue over people's needs and interests.

Instead, there is competition and diversity of digital services for users to choose from, and these services use interoperable architectures that enable users to switch easily to other providers and mix-and-match services of their choice within the same platform. For example, third-party providers create products that enable users to seamlessly communicate on social media channels from a standalone app. Large platforms allow their users to change the default content curation algorithm to the one of their choice.

Thanks to full horizontal and vertical interoperability, people using digital services are empowered to choose their favourite or trusted provider of infrastructure, content and interface. Rather than platforms setting rules and objectives that determine what information is surfaced by their recommender system, third-party providers, including reputable news organisations and non-profits, can build customised filters (operating on the top of default recommender systems to modify the newsfeed) or design alternative recommender systems.

All digital platforms and service providers operate within high standards of security and protection, which are audited and enforced by national regulators. Following new regulatory requirements, large platforms operate under standard protocols that are designed to respect choices made by their users, including strict limitations on the use of their personal data.

How to get from here to there

In today's digital markets, there is unprecedented consolidation of power in the hands of a few, large US and Chinese digital companies. This tendency towards centralised power is supported by the current abilities of platforms to:

- process substantial quantities of personal and non-personal data, to optimise their services and the experience of each business or individual user
- extract market-dominating value from large-volume interactions and transactions
- use their financial power to either acquire or imitate (and further improve) innovations in the digital economy
- use this capacity to leverage dominance into new markets
- use financial power to influence legislation and stall enforcement through litigation.

The table on page 41 takes a more detailed look at some of the sources of power and possible remedies.

These dynamics reduce the possibility for new alternative services to be introduced and contribute to users' inability to switch services and to make value-based decisions (for example, to choose a privacy-optimised social media application, or to determine what type of content is prioritised on their devices).[74] Instead, a few digital platforms have the ability to capture a large user base and extract value from attention-maximising algorithms and 'dark patterns' – deceptive design practices that influence users' choices and encourage them to take actions that result in more profit for the corporation, often at the expense of the user's rights and digital wellbeing.[75]

As discussed in Chapter 1, there is still much to explore when considering possible regulatory solutions, and there are many possible approaches to reducing concentration and market dominance. Conceptual discussions about regulating digital platforms that have been promoted in policy and academia range from 'breaking up big tech',[76] by separating the different services and products they control into separate companies, to nationalising and transforming platforms into public utilities or conceiving of them as universal digital services.[77] Alternative proposals suggest limiting the number of data-processing activities a company can perform concurrently, for example separating search activities from targeted advertising that exploits personal profiles.

There is a need to go further. The imaginary picture painted at the start of this section points towards an environment where there is competition and meaningful choice in the digital ecosystem, where rights are more rigorously upheld and where power over infrastructure is less centralised. This change in power dynamics would require, as one of the first steps, that digital infrastructure is transformed with full vertical and horizontal interoperability. The imagined ecosystem includes large online platforms, but in this scenario they find it much more difficult to maintain a position of dominance, thanks to real-time data portability, user mobility and requirements for interoperability stimulating real competition in digital services.

What is interoperability?

Interoperability is the ability of two or more systems to communicate and exchange information. It gives end users the ability to move data between services (data portability), and to access services across multiple providers.

How can interoperability be enabled?

Interoperability can be enabled by developing (formal or informal) standards that define a set of rules and specifications that, when implemented, allow different systems to communicate and work together. Open standards are created through the consensus of a group of interested parties and are openly accessible and usable by anyone.

This section explores a range of interoperability measures that can be introduced by national or European policy makers, and discusses further considerations to transform the current, closed platform infrastructure into an open ecosystem.

Introducing platform interoperability

Drawing from examples of other sectors that historically have operated in silos, mandatory interoperability measures are a potential tool that merit further exploration, to create new opportunities for both companies and users.

Interoperability is a longstanding policy tool in EU legislation and more recent digital competition reviews suggest it as a measure against highly concentrated digital markets.[78]

In telecommunications, interoperability measures make it possible to port phone numbers from one provider to another, and enable customers of one phone network to call and message customers on other networks, improving choice for consumers. In the banking sector, interoperability rules made it possible for third parties to facilitate account transfers from one bank to another, and to access data about account transactions to build new services. This opened up the banking market for new competitors and delivered new types of financial services for customers.

In the case of large digital platforms, introducing **mandatory interoperability measures** is one way to allow more choice of service (preventing both individual and business users from being trapped in one company's products and services), and to re-establish the conditions to enable a competitive market for start-ups and small and medium-sized enterprises to thrive.[79]

While some elements of interoperability are present in existing or proposed EU legislation, this section explores a much wider scope of interoperability measures than those that have already been adopted. (For a more detailed discussion on 'Possible interoperability mandates and their practical implications', see the text box below.)

Some of these elements of interoperability in existing or proposed EU legislation are:[80]

- The Digital Markets Act enables interoperability requirements between instant messaging services, as well as with the gatekeepers' operating system, hardware and software (when the gatekeeper is providing complementary or supporting services), and strengthens data portability rights.[81]
- The Data Act proposal aims to enable switching between cloud providers.[82]
- Regulation on promoting fairness and transparency for business users of online intermediation services ('platform-to-business regulation') gives business users the right to access data generated through the provision of online intermediation services.[83]

These legislative measures address some aspects of interoperability, but place limited requirements on services other than instant messaging services, cloud providers and operating systems in certain situations.[84] They also do not articulate a process for creating technical standards around open protocols for other services. This is why there is a need to test more radical ideas, such as mandatory interoperability for large online platforms covering both access to data and platform functionality.

In the case of large digital platforms, introducing mandatory interoperability measures is one way to allow more choice of service (preventing both individual and business users from being trapped in one company's products and services), and to re-establish the conditions to enable a competitive market for start-ups and small and medium-sized enterprises to thrive.

Possible interoperability mandates and their practical implications

Ian Brown

Interoperability in digital markets requires some combination of **access to data** and **platform functionality**.

Data interoperability

Data portability (Article 20 of the EU GDPR) is the right of a user to move their personal data from one company to another. (The Data Transfer Project developed by large technology companies is slowly developing technical tools to support this.)[85] This should help an individual switch from one company to another, including by giving price comparison tools access to previous customer bills.

However, a wider range of uses could be enabled by real-time data mobility[86] or interoperability,[87] implying that an individual can give one company permission to access their data held by another, and meaning it can be updated whenever they use the second service. These remedies can stand alone, where the main objective is to enable individuals to give access to their personal data held by an incumbent firm to competitors. Scholars make an additional distinction between syntactic or technical interoperability, the ability for systems to connect and exchange data (often via Application Programming Interfaces or 'APIs') and semantic interoperability, that connected systems share a common understanding of the meaning of data they exchange.[88]

An important element of making both types of data-focused interoperability work is developing more data standardisation to require datasets to be structured, organised, stored and transmitted in more consistent ways across different devices, services and systems. Data standardisation creates common ontologies, or classifications, that specify the meaning of data.[89]

For example, two different instant messaging services would benefit from a shared internal mapping of core concepts such as identity (phone number, nickname, email), rooms (public or private group chats, private messaging), reactions, attachments, etc. – these are concepts and categories that could be represented in a common ontology, to bridge functionality and transfer data across these services.[90]

Data standardisation is an essential underpinning for all types of portability and interoperability and, just like the development of technical standards for protocols, it needs both industry collaboration and measures to ensure powerful companies do not hijack standards to their own benefit.

An optional interoperability function is to require companies to support personal data stores (PDS), where users store and control data about them using a third-party provider and can make decisions about how it is used (e.g. the MyData model,[91] and Web inventor Tim Berners-Lee's Solid project).

The data, or consent to access it, could be managed by regulated aggregators (major Indian banks are developing a model where licensed entities aggregate account data with users' consent and therefore act as an interoperability bridge between multiple financial services),[92] or facilitated by user software through an open set of standards adopted by all service providers (as in the UK's Open Banking). It is also possible for service providers to send privacy-protective queries or code to run on personal data stores inside a protected sandbox, limiting the service provider's access to data (e.g. a mortgage provider could send code, checking an applicant's monthly income was above a certain level, to their PDS or current account provider, without gaining access to all of their transaction data).[93]

The largest companies currently have a significant advantage in their access to very large quantities of user data, particularly when it comes to training machine learning systems. Requiring access to statistical summaries of the data (e.g. popularity of specific social media content and related parameters) may be sufficient, while limiting the privacy problems caused. Finally, firms could be required to share the (highly complex) details of machine learning models, or provide regulators and third-parties access to them to answer specific questions (such as the likelihood a given piece of social-media content is hate speech).

The interoperability measures described above would enable a smoother transfer of data between digital services, and enable users to exert more control over what kind of data is shared and in what circumstances. This would make for a 'cleaner' data ecosystem, in which platforms and services are no longer incentivised to gather as much data as possible on every user.

Rather, users would have more power to determine how their data is collected and shared, and smaller services wouldn't need to engage in extractive data practices to 'catch up' with larger platforms, as barriers to data access and transfer would be reduced. The overall impact on innovation would depend on whether increased competition resulting from data sharing at least counterbalanced these reduced incentives.

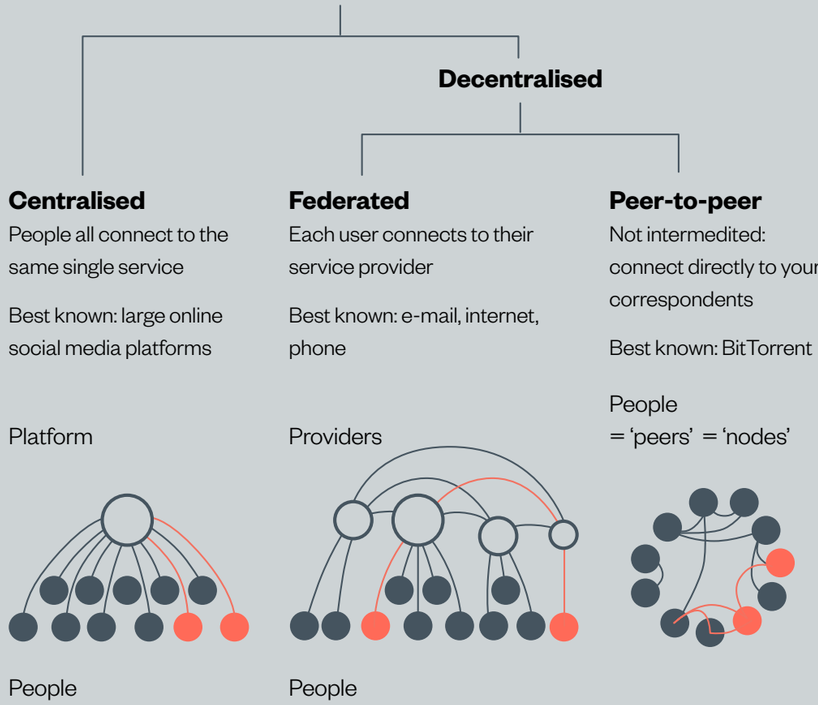
Functionality-oriented interoperability

Another form of interoperability relates to enabling digital services and platforms to work cross-functionally, which could improve user choice in the services they use and reduce the risk of 'lock in' to a particular service. Examples of functionality-oriented interoperability (sometimes referred to as protocol interoperability,[94] or in telecoms regulation, interconnection of networks) include:

- the ability for a user of one instant-messaging service to send a message to a user or group on a competing service
- the user of one social media service can 'follow' a user on another service, and 'like' their shared content
- the ability of a user of a financial services tool to initiate a payment from an account held with a second company
- the user of one editing tool can collaboratively edit a document or media file with the user of a different tool, hosted on a third platform.

Services communicate with each other using open/publicly accessible APIs and/or standardised protocols. In Internet services, this generally looks like the 'decentralised' network architectures shown below:

Network architectures



The UK's Open Banking Standard recommended: 'The Open Banking API should be built as an open, federated and networked solution, as opposed to a centralised/hub-like approach. This echoes the design of the Web itself and enables far greater scope for innovation.'[95]

An extended version of functional interoperability would allow users to exercise other forms of control over the products and services they use, including:

- signalling their preferences to platforms on profiling – the recording of data to assess or predict their preferences – using a tool such as the Global Privacy Control, or expressing their preferred default services such as search
- replacing core platform functionality, such as a timeline ranking algorithm or an operating system default mail client, with a preferred version from a competitor (known as modularity)[96]
- using their own choice of software to interact with the platform.

Noted competition economist Cristina Caffarra has concluded: 'We need wall-to-wall [i.e. near-universal] interoperability obligations at each pinch point and bottleneck: only if new entrants can connect and leverage existing platforms and user bases can they possibly stand a chance to develop critical mass.'[97] Data portability alone is a marginal solution (and a limited remedy for GAFAM (Google, Apple, Facebook (now Meta Platforms), Amazon, Microsoft) when those companies want to flag their good intentions.[98] A review of portability in the Internet of Things sector came to a similar conclusion.[99]

Further considerations and provocative concepts

Mandatory interoperability measures have the potential to transform digital infrastructure, and to enable innovative services and new experiences for users. However, they need to be supported by carefully considered additional regulatory measures, such as cybersecurity, data protection and related accountability frameworks. (See text box below on 'How to address sources of platform power? Possible remedies' for an overview of interoperability and data protection measures that could tackle some of the sources of power for platforms.)

Also, the development of technical standards for protocols and classification systems or ontologies specifying the meaning of data (see text box above on 'Possible interoperability mandates and their practical implications') is foundational to data and platform interoperability. However, careful consideration must be placed on designing new types of infrastructure, in order to prevent platforms from consolidating control. Examples from practice show that developing open standards and protocols are not enough on their own.

Connected to the example above on signalling preferences to platforms, open protocols such as the 'Do Not Track' header were meant to help users more easily exercise their data rights by signalling an opt-out preference from website tracking.[100] In this case, the standardisation efforts stopped due to insufficient deployment,[101] demonstrating the significant challenge in obliging platforms to facilitate the use of standards in the services they deploy.

A final point relates to creating interoperable systems that do not overload users with too many choices. Already today it is difficult for users to manage all the permissions they give across all the services and platforms they use. Interoperability may offer solutions for users to share their preferences and permissions for how their data should be collected and used by platforms, without requiring recurring 'cookie notice'-type requests to a user when using each service.

How to address sources of platform power? Possible remedies

Ian Brown

Interoperability and related remedies have the potential to address not only problems resulting from market dominance of a few large firms, but – more importantly – some of the sources of their market power. However, every deep transformation needs to be carefully designed to prevent unwanted effects. The challenges associated with designing market interventions based on interoperability mandates need to be identified early in the policy- making process so that problems can either be solved or accounted for.

The table below presents specific interoperability measures, classified by their potential to address various sources of large platforms' power, next to problems that are likely to result from their implementation.

While much of the policy debate so far on interoperability remedies has taken place within a competition-law framework (including telecoms and banking competition), there are equally important issues to consider under data and consumer protection law, as well as useful ideas from media regulation. Competition-focused measures are generally applied only to the largest companies, while other measures can be more widely applied. In some circumstances these measures can be imposed under existing competition-law regimes on dominant companies in a market, although this approach can be extremely slow and resource-intensive for enforcement agencies.

The EU Digital Markets Act (DMA), and US proposals (such as the ACCESS Act and related bills), impose some of these measures up-front on the very largest 'gatekeeper' companies (as defined by the DMA). The European Commission has also introduced a Data Act that includes some of the access to data provisions below.[102] Under these measures, smaller companies are free to decide whether to make use of interoperability features that their largest competitors may be obliged to support.

Sources of market power for large firms/platforms	Proposed interoperability or related remedies	Potential problems
Access to individual customer data (including cross-use of data from multiple services)	Real-time and continuous user-controlled data portability/data interoperability Requirement to support user data stores (Much) stricter enforcement of data minimisation and purpose limitation requirements under data protection law, alongside meaningful transparency about reasons for data collection (or prohibiting certain data uses cross-platform)	Need for multiple accounts with all services, and take-it-or-leave-it contract terms Incentive for mass collection, processing and sharing of data, including profiling
Access to large-scale raw customer data for analytics/product improvement	Mandated competitor access to statistical data[103] **Mandated competitor access to raw data is dismissed because of significant data protection issues*	Reduced incentives for data collection
Access to large-scale aggregate/ statistical customer data	Mandated competitor access to models, or specific functionality of models via APIs	Reduced incentives for data collection and model training
Ability to restrict competitor interaction with customers	Requirement to support open/publicly accessible APIs or standardised communications protocols	Complexity of designing APIs/ standards, while preventing anticompetitive exclusion
Availability and use of own core platform services to increase 'stickiness'	Government coordination and funding for development of open infrastructural standards and components Requirement for platforms to support/integrate these standard components	Technical complexity of full integration of standard/competitor components into services/design of APIs while preventing anticompetitive exclusion Potential pressure for incorporation of government surveillance functionality in standards
Ability to fully control user interface, such as advertising, content recommendation, specific settings, or self-preferencing own services	Requirement to support competitors' monetisation and filtering/ recommendation services via open APIs[104] Requirement to present competitors' services to users on an equal basis[105] Requirement to recognise specific user signals Open APIs to enable alternative software clients	Technical complexity of full integration of competitor components into services/design of APIs while preventing anticompetitive exclusion

Food for thought

In the previous section strong data protection and security provisions were emphasised as essential for building an open ecosystem that enables more choice for users, respects individual rights and facilitates competition.

Going a step further, there is a discussion to be had about boundaries of system transformation that seem achievable with interoperability. What are the 'border' cases, where the cost of transformation outweighs its benefits? What immediate technical, societal and economic challenges can be identified, when imagining more radical implementations of interoperability than those that have already been tested or are being proposed in EU policy?

In order to trigger further discussion, a set of problems and questions are offered as provocations:

1. **Going further, imagine a fully interoperable ecosystem, where different platforms can talk to each other.** What would it mean to apply a full interoperability mandate across different digital services and what opportunities would it bring? For example, provided that technical challenges are overcome, what new dynamics would emerge if a Meta Platforms (Facebook) user could exchange messages with Twitter, Reddit or TikTok users without leaving the platform?

2. **More modular and customisable platform functionalities may change dynamics between users and platforms and lead to new types of ecosystems.** How would the data ecosystem evolve if core platform functionalities were opened up? For example, if users could choose to replace core functionalities such as content moderation or news feed curation algorithms with alternatives offered by independent service providers, would this bring more value for individual users and/or societal benefit, or further entrench the power of large platforms (becoming indispensable infrastructure)? What other policy measures or economic incentives can complement this approach in order to maximise its transformative potential and prevent harms?

3. **Interoperability measures have produced important effects in other sectors and present a great potential for digital markets.** What lessons can be learned from introducing mandatory interoperability in the telecommunications and banking sectors? Is there a recipe for how to open up ecosystems with a 'people-first' approach that enables choice while preserving data privacy and security, and provides new opportunities and innovative services that benefit all?

4. **Interoperability rules need to be complemented and supported by measures that take into account inequalities and make sure that the more diverse portfolio of services that is created through interoperability is accessible to the less advantaged.** Assuming more choice for consumers has already been achieved through interoperability mandates, what other measures need to be in place to reduce structural inequalities that are likely to keep less privileged consumers locked in the default service? Experience from the UK energy sector shows that it is often the consumers/users with the fewest resources who are least likely to switch services and benefit from the opportunity of choice (the 'poverty premium').[106]

2. Reclaiming control of data from dominant companies

The vision

In this world, the primary purpose of generating, collecting, using, sharing and governing data is to create value for people and society. The power to make decisions about data has been removed from the few large technology companies who controlled the data ecosystem in the early twenty-first century, and is instead delegated to public institutions with civic engagement at a local and national level.

To ensure that data creates value for people and society, researchers and public-interest bodies oversee how data is generated, and are able to access and repurpose data that traditionally has been collected and held by private companies. This data can be used to shape economic and social policy, or to undertake research into social inequalities at the local and national level. Decisions around how this data is collected, shared and governed are overseen by independent data access boards.

The use of this data for societally beneficial purposes is also carefully monitored by regulators, who provide checks and balances on both private companies to share this data under high standards of security and privacy, and on public agencies and researchers to use that data responsibly.

In this world, positive results are being noticed from practices that have become the norm, such as developers of data-driven systems making their systems more auditable and accessible to researchers and independent evaluators. Platforms are now fully transparent about their decisions around how their services are designed and used. Designers of recommendation systems publish essential information, such as the input variables and optimisation criteria used by algorithms and results of their impact assessments, which supports public scrutiny. Regulators, legislators, researchers, journalists and civil society organisations easily interrogate algorithmic systems, and have a straightforward understanding over what decisions systems may be rendering and how those decisions impact people and society.

Finally, national governments have launched 'public-interest data companies', which collect and use data under strict requirements for objectives that are in the public interest. Determining 'public interest' is a question these organisations routinely return to through participatory exercises that empower different members of society.

The importance of data in the digital market triggers the question how control over data and algorithms can be shifted away from dominant platforms, to allow individuals and communities to be involved in decisions about how their data is used. The imaginary scenario above builds a picture of a world where data is used for public good, and not (only) for corporate gain.

Current exploitative data practices are based on access to large pools of personal and non-personal data and the capacity to efficiently use data to extract value by means of advanced analytics.[107] The insights into social patterns and trends that are gained by large companies through analysing vast datasets currently remain closed off and are used for extracting and maximising commercial gains, where they could have considerable social value.

Determining what constitutes uses of data for 'societal benefit' and 'public interest' is a political project that must be undertaken with due regard for transparency and accountability. Greater mandates to access and share data must be accompanied by strict regulatory oversight and community engagement to ensure these uses deliver actual benefit to individuals impacted by the use of this data.

The previous section discussed the need to transform infrastructure in order to rebalance power in the digital ecosystem. Another and interrelated foundational area where more profound legal and institutional change is needed is in control over data.

Why reclaim control over data?

For the purposes of this proposition, reflecting the focus on creating more societal benefit, the first goal of reclaiming control over data is to open up access to data and resources from companies and repurposing them for public-interest goals, such as developing public policies that take into consideration insights and patterns from large-scale datasets. A second purpose is to open up access to data and to machine-learning algorithms, in order to increase scrutiny, accountability and oversight over how proprietary algorithms function and to understand their impact at the individual, collective and societal level.

How to get from here to there

Proprietary siloing of data is currently one of the core obstacles to using data in societally beneficial ways. But simply making data more shareable, without specific purposes and strong oversight can lead to greater abuses rather than benefits. To counter this, there is a need for:

- legal mandates that private companies make data and resources available for public interest purposes
- regulatory safeguards to ensure this data is shared securely and with independent oversight.

Mandating companies share data and resources in the public interest

One way to reclaim control over data and repurpose it for societal benefits is to create legal mandates requiring companies to share data and resources that could be used in the public interest. For example:

- **Mandating the release from private companies of personal and non-personal aggregate data for public use** (where aggregate data means a combination of individual data, which is anonymised through eliminating personal information).[108] These datasets would be used to inform public policies (e.g. use mobility patterns from a ride-sharing platform to develop better road infrastructure and traffic management).[109]

- **Requiring companies to create interfaces for running data queries on issues of public interest** (for example public health, climate, pollution, etc). This model relies on using the increased processing and analytics capabilities inside a company, instead of asking for access to large 'data dumps', which might prove difficult and resource intensive for public authorities and researchers to process. Conditions need to be in place around what types of queries are allowed, who can run these and what are the company's obligations around providing responses.

- **Providing access for external researchers and regulators to machine learning models and core technical parameters of AI systems**, which could enable evaluation of an AI system's performance and real optimisation goals (for example checking the accuracy and performance of content moderation algorithms for hate speech).

Some regulatory mechanisms are emerging at national and regional level in support of data access mandates. For example, in France, the 2016 Law for a Digital Republic (*Loi pour une République numérique*) introduces the notion of 'data of general interest' which includes access to data from private entities that have been delegated to run a public service (e.g. utility or transportation), access to data from entities whose activities are subsidised by public authorities, and access to certain private databases for the statistical purposes.[110]

In Germany, the 2019 leader of the Social Democratic Party championed a 'data for all' law that advocated for a 'data commons' approach and breaking-up data monopolies through a data-sharing obligation for market-dominant companies.[111] In the UK, the Digital Economy Act provides a legal framework for the Office for National Statistics (ONS) to access data held within the public and private sectors in support of statutory functions to produce official statistics and statistical research.[112]

The EU's Digital Services Act (DSA) includes a provision on data access for independent researchers.[113] Under the DSA, large companies will need to comply with a number of transparency obligations, such as creating a public database of targeted advertisement and providing more transparency around how recommender systems work. It also includes an obligation for large companies to perform systemic risk assessments and to implement steps to mitigate risk.

In order to ensure compliance with the transparency provisions in the regulation, the DSA mandates independent auditors and vetted researchers with access to the data that led to the company's risk assessment conclusions and mitigation decisions. This provision ensures oversight over the self-assessment (and over the independent audit) that companies are required to carry out, as well as scrutiny over the choices large companies make around their systems.

Other dimensions of access to data mandates can be found in the EU's Data Act proposal, which introduces compulsory access to company data for public-sector bodies in exceptional situations (such as public emergencies or where it is needed to support public policies and services).[114] The Data Act also provides for various data access rights, such as a right for individuals and businesses to access the data generated from the products or related service they use and share the data with a third party continuously and in real-time[115] (companies which fall under the category of 'gatekeepers' are not eligible to receive this data [116]).

This forms part of the EU general governance framework for data sharing in business-to-consumer, business-to-business and business-to-government relationships created by the Data Act. It complements the recently adopted Data Governance Act (focusing on voluntary data sharing by individuals and businesses and creating common 'data spaces') and the Digital Markets Act (which strengthens access by individual and business users to data provided or generated through the use of core platform services such as marketplaces, app stores, search, social media, etc.).[117]

Independent scrutiny of data sharing and AI systems

Sharing data for the 'public interest' will require novel forms of independent scrutiny and evaluation, to ensure such sharing is legitimate, safe, and has positive societal impact. In cases where access to data is involved, concerns around privacy and data security need to be acknowledged and accounted for.

In order to mitigate some of these risks, one recent model proposes a system of governance in which a new independent entity would assess the researchers' skills and capacity to conduct research within ethical and privacy standards.[118] In this model, an independent ethics board would review the project proposal and data protection practices for both the datasets and the people affected by the research. Companies would be required to 'grant access to data, people, and relevant software code in the form researchers need' and refrain from influencing the outcomes of research or suppressing findings.[119]

An existing model for gaining access to platform data is Harvard's SocialScienceOne project,[120] which partnered with Meta Platforms (Facebook) in the wake of the Cambridge Analytica scandal to control access to a dataset containing public URLs shared and clicked by Facebook users globally, along with metadata including Facebook likes. Researchers requests for access to the dataset go to an academic advisory board that is independent from Facebook, and which reviews and approves applications.

While initiatives like SocialScienceOne are promising, it has faced its share of criticism for failing to provide timely access to requests,[121] and concerns that the dataset Meta Platforms (Facebook) shared has significant gaps.[122] The programme also relies on the continued voluntary action of Meta Platforms (Facebook), and therefore lacks any guarantees that the corporation (or others like it) will provide this data in years to come. Future regulatory proposals should explore ways to create incentives for firms to share data in a privacy-preserving way, but not use them as shields and excuses to prevent algorithm inspection.

A related challenge is developing novel methods for ensuring external oversight and evaluation of AI systems and models that are trained on data shared in this way. Two approaches to holding platforms and digital services accountable to the users and communities they serve are algorithmic impact assessments, and algorithm auditing.

Algorithmic impact assessments look at how to identify possible societal impacts of a system before it is in use, and ongoing once it is. They have been proposed primarily in the public sector,[123] with a focus on public participation in the identification of harms and publication of findings. Recent work has seen them explored in a data access context, making them a condition of access. [124]

Algorithm auditing involves looking at the behaviour of an algorithmic system (usually by examining inputs and outputs) to identify whether risks and potential harms are occurring, such as discriminatory outcomes,[125] or the prevalence of certain types of content.[126]

The Ada Lovelace Institute's work identified six technical inspection methods that could be applied in scrutinising social media platforms, each with its own limitations and challenges.[127] Depending on the method used, access to data is not always necessary, however important elements for enabling auditing are: access to documentation about the dataset's structure and purpose, the system's design and functionality, and access to interviews with developers of that system.

In recent years, a number of academic and civil society initiatives to conduct third-party audits of platforms have been blocked because of barriers to accessing data held by private developers. This has led to repeated calls for increased transparency and access to the data that platforms hold.[128] [129]

There is also growing interest in the role of regulators, who, in a number of jurisdictions, will be equipped with new inspection and information-gathering powers over social media and search platforms, which could overcome access challenges experienced by research communities.[130] One way forward may be for regulators to have the power to issue 'access to platform data' mandates for independent researchers, who can collect and analyse data about potential harms or societal trends under strict data protection and security conditions, for example minimising the type of data collected and with a clear data retention policy.

Further considerations and provocative concepts

Beyond access to data: grappling with fundamental issues

Jathan Sadowski

To reclaim resources and rights currently controlled by corporate platforms and manage them in the public's interests and for societally beneficial purposes, 'a key enabler would be a legal framework mandating private companies to grant access to data of public interest to public actors under conditions specified in the law.'[131] One aspect that needs to be considered is whether this law should establish requirements around data collected by large companies to become part of the public domain after a reasonable number of years.

Another proposal suggested the possibility of allowing companies to use the data that they gather only for a limited period (e.g. five years), after which it is reverted to a 'national charitable corporation that provides access to certified researchers, who would both be held to account and be subject to scrutiny to ensure the data is used for the common good'.[132]

These ideas will have to consider various issues, such as the need to ensure that individual's data is not released into the public domain, and the fact that commercial competitors might not see any benefit in using 'old' data. Nevertheless, we should draw inspiration from these efforts and seek to expand their purview.

To that point, policies aimed at making data held by private companies into a common resource should go further than simply allowing other companies to access data and build their own for-profit products from it. To rein in the largely unaccountable power of big technology companies who wield enormous, and often black-boxed, influence over people's lives,[133] these policies must grapple with fundamental issues related to who gets to determine how data is made, what it means, and why it is used.

Furthermore, the same policies should extend their target beyond monopolistic digital platforms. Data created and controlled by, for example, transportation services, energy utilities and credit rating agencies ought also to be subjected to public scrutiny and democratic decisions about the most societally beneficial ways to use it or discard it.

Further to these considerations, in this section provocative concepts are shared, which show different implementation models that can be set up in practice to re-channel the use of data and resources from companies towards societal good.

Public interest divisions with public oversight

Building on the Uber Movement model, which releases aggregate datasets on a restricted, non-commercial basis to help cities with urban planning,[134] relevant companies could be obliged to form a well-resourced public interest division, running as part of the core organisational structure with full access to the company's capabilities (such as computational infrastructure and machine learning models).

This division would be in charge of building aggregate datasets to support important public value. Key regulators could issue 'data-sharing mandates', to identify which types of datasets would be most valuable and run queries against them. Through this route, the computational resources and the highly skilled human resources of the company would be used for achieving societal benefits and informing public policy.

The aggregate datasets could be used to inform policymaking and public service innovation. Potential examples could include food delivery apps informing health nutrition policies, or ride-sharing apps informing street planning, traffic congestion, housing and environmental policies. There would be limitations to use: for example insights from social media companies could be used for identifying the most pressing social issues in one area, and this information should not be used by the political class in the electoral cycle or for winning popularity by gaining political insight and using it in political campaigns.

Publicly run corporations (the 'BBC for data')

Another promising avenue for repurposing data in the public interest and increasing accountability is to introduce a publicly run competitor to specific digital platforms (e.g. social media). This model could be established by mandating the sharing of data from particular companies operating in a given jurisdiction to a public entity, which uses the data for projects that are in service of the public good.[135]

The value proposition behind such an intervention in the digital market would be similar to the effect of the British Broadcasting Corporation (BBC) in the UK broadcast market, where it competes with other broadcasters. The introduction of the BBC supported competition in dimensions other than audience numbers, and provided a platform for more types of content providers (for example music and independent production) that otherwise may not have existed, or not at a scale enabling them to address global markets.

Operating as a publicly run corporation has the benefit of establishing a different type of incentive structure, one that is not narrowly focused on profit-making. This could avoid the more extractive, commercially oriented business models and practices that result from the need to generate profits for shareholders and demonstrate continuous growth.

One business model that dominates the digital ecosystem, and is the primary incentive for many of the largest technology companies, is online advertising. This model has underpinned the development of mature, developed platforms, which means that, while individuals may support the concept of a business model that does not rely on extractive practices, in practice it may be difficult to get users to switch to services that do not offer equivalent levels of convenience and functionality. The success of this model is dependent on the 'BBC for data' competitor offering broad appeal and well-designed, functional services, so it can scale to operate at a significant level in the market.

The introduction of a democratically accountable competitor alone would not be enough to shape new practices, or to establish political and public support. It would need committed investment in the performance of its services and in attracting users. Citizens should be engaged in shaping the practices of the new public competitor, and these should reflect – in market terms – what choices, services and approaches they expect.

Food for thought

As argued above, reclaiming control over data and resources to public authorities, researchers, civil society organisations and other bodies that work in the public interest has a transformative potential. The premise of this belief is simple: if data is power, making data accessible to new actors, with non-commercial goals and agendas, will shift the power balance and change the dynamic within the data ecosystem. However, without deeper questioning, the array of practical problems and structural inequalities will not disappear with the arrival of new actors and their powers to access data.

Enabling data sharing is no simple feat – it will require extensive consideration of privacy and security issues, and oversight from regulators to prevent the misuse, abuse or concealing of data. The introduction of new actors and powers to access and use data will, inevitably, trigger other externalities and further considerations that are worthy of greater attention from civil society, policymakers and practitioners.

In order to trigger further discussion, a set of problems and questions are offered as provocations:

1. **Discussions around 'public good' need mechanisms to address questions of legitimacy and accountability in a participatory and inclusive way**. Who should decide what uses of data serve the public good and how these decisions should be reached in order to maintain their legitimacy as well as social accountability? Who decides what constitutes 'public good' or 'societal benefit,' and how can such decisions be made justly?

2. **Enabling data sharing and access needs to be accompanied by robust privacy and security measures**. What legal requirements and conditions need to be designed for issuing 'data sharing' mandates from companies?

3. **Data sharing and data access mandates imply that the position of large corporations is still a strong one, and they are still playing a substantial role in the ecosystem**. In what ways might data-sharing mandates entrench the power of large technology platforms, or exacerbate different kinds of harm? What externalities are likely to arise with mandating data sharing for public interest goals from private companies?

4. **The notion of 'public good' opens important questions about what type of 'public' is involved in discussions and who gets left out**. How can determinations of public good be navigated in inclusive ways across different jurisdictions, and accounting for structural inequalities?

To rein in the largely unaccountable power of big technology companies who wield enormous – and often black-boxed – influence over people's lives, these policies must grapple with fundamental issues related to who gets to determine how data is made, what it means and why it is used.

3. Rebalancing the centres of digital power with new (non-commercial) institutions

The vision

In this world, new forms of data governance institutions made up of collectives of citizens control how data is generated, collected, used and governed. These intermediaries, such as data trusts and data cooperatives, empower 'stewards' of data to collect and use data in ways that support their beneficiaries (those represented in and affected by that data).

These models of data governance have become commonplace, enabling people to be more aware and exert more control over who has access to their data, and engendering a greater sense of security and trust that their data will only be used for purposes that they approve.

Harmful uses of data are more easily identifiable and transparent, and efficient forms of legal redress are available in cases where a data intermediary acts against the interests of their beneficiary.

The increased power of data collectives balances the power of dominant platforms, and new governance architectures offer space for civil society organisations to hold to account any ungoverned or unregulated, private or public exercises of power.

There is a clear supervision and monitoring regime ensuring 'alignment' to the mandate that data intermediaries have been granted by their beneficiaries. Data intermediaries are discouraged and prevented from monetising data. Data markets have been prohibited by law, understanding that the commodification of data creates room for abuse and exploitation.

The creation and conceptualisation of new institutions that manage data for non-commercial purposes is necessary to reduce power and information asymmetries.

Large platforms and data brokers currently collect and store large pools of data, which they are incentivised to use for corporate rather than societal benefit. Decentring and redistributing the concentration of power away from large technology corporations and towards individuals and collectives requires explorations around new ways of governing and organising data (see the text box on 'Alternative data governance models' below).

Alternative data governance models could offer a promising pathway for ensuring data subjects have rights and preferences over how their data is used are enforced. If designed properly, these governance methods could also help to address structural power imbalances. However, until power is shifted away from large companies, and market dynamics are redressed to allow more competition and choice, there is a high risk of data intermediaries being captured.

New vehicles representing collective power, such as data unions, data trusts, data cooperatives or data-sharing initiatives based on corporate or contractual mechanisms, could help individuals and organisations position themselves better in relation to more powerful private or public organisations, offering new possibilities for enabling choices related to how data is being used.[136]

There are many ways in which these models can be set up. For example, some models put more emphasis on individual gains, such as a 'data union' or a data cooperative that works in the individual interest of its members (providing income streams for individuals who pool their personal data, which is generated through the services they use or available on their devices).

These structures can also work towards wider societal aspirations, when members see this as their priority. Another option might be for members to contribute device-generated data to a central database, with ethically minded entrepreneurs invited to build businesses on top of these databases, owned collectively by the 'data commons' and feeding its revenues back into the community, instead of to the individual members.

A detailed discussion on alternative data governance models is presented in the Ada Lovelace Institute report Exploring legal mechanisms for data stewardship, which discusses three legal mechanisms – data trusts, data cooperatives, and corporate and contractual mechanisms – that could help facilitate the responsible generation, collection, use and governance of data in a participatory and rights-preserving way.[137]

Alternative data governance models

- **Data trusts:** stemming from the concept of UK trust law, individuals pool data rights (such as those provided by the GDPR) into an organisation – a trust – where the data trustees are tasked with exercising data rights under fiduciary obligations.
- **Data cooperatives:** individuals voluntarily pool data together, and the benefits are shared by members of the cooperative. A data cooperative is distinct from a 'data commons' because a data cooperative grows or shrinks as resources are brought in or out (as members join or leave), whereas a 'data commons' implies a body of data whose growth or decline is independent of the membership base.
- **Corporate and contractual agreements:** legally binding agreements between different organisations that facilitate data sharing for a defined set of aims or an agreed purpose.

Many of the proposed models for data intermediaries need to be tested and further explored to refine their practical implementation, and the considerations below offer a more critical perspective highlighting how the different transformations of the data ecosystem discussed in this chapter are interconnected, and how one institutional change (or failure) determines the conditions for a change in another area.

Decentralised intermediaries need adequate political, economic, and infrastructural support, to fulfil their transformative function and deliver the value expected from them. The text box below, by exploring the shortcomings of existing data intermediaries, gives an idea of the economic and political conditions that would provide a more enabling environment.

Until power is shifted away from large companies, and market dynamics are redressed to allow more competition and choice, there is a high risk of data intermediaries being captured.

Critical overview of existing data intermediaries models

Jathan Sadowski

There are now a number of emerging proposals for alternative data intermediaries that seek to move away from the presently dominant, profit-driven model and towards varying degrees of individual ownership, legal oversight or social stewardship of data.[138]

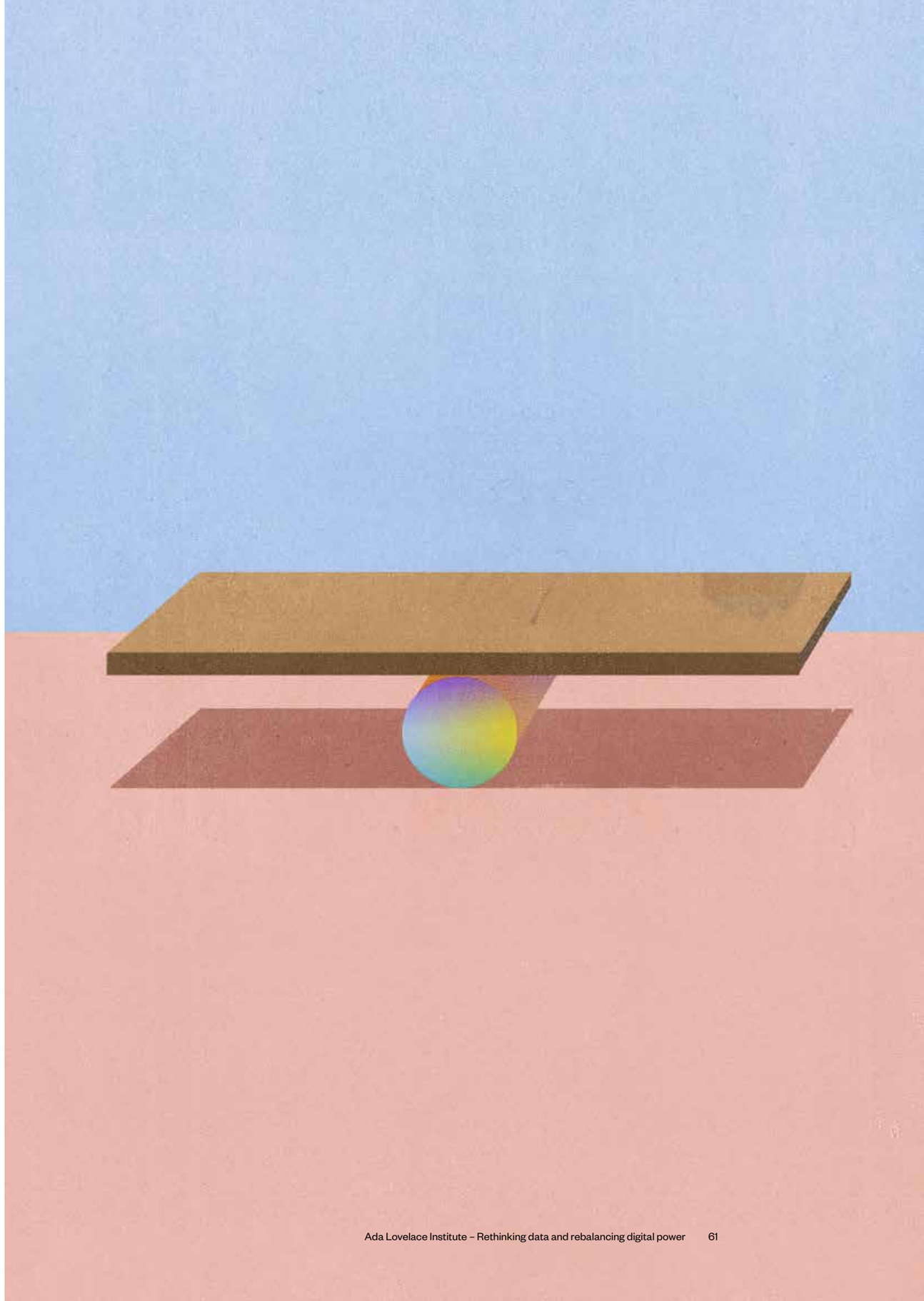
These proposals include relatively minor reforms to the status quo, such as legally requiring companies to act as 'information fiduciaries' and consider the interests of stakeholders who are affected by the company, alongside the interests of shareholders who have ownership in the company.

In a recent Harvard Law Review article, David Pozen and Lina Khan[139] provide detailed arguments for why designating a company like Meta Platforms (Facebook) – 'a loyal caretaker for the personal data of millions' does not actually pose a serious challenge to the underlying business model or corporate practices. In fact, such reforms may even entrench the company's position atop the economy. 'Facebook-as-fiduciary is no longer a public problem to be solved, potentially through radical reform. It is a nexus of sensitive private relationships to be managed, nurtured, and sustained [by the government]'.[140]

Attempts to tweak monopolistic platforms, without fundamentally restructuring the institutions and distributions of economic power, are unlikely to produce – and may even impede – the meaningful changes needed.

Other models take a more decentralised solution in the form of 'data-sharing pools'[141] and 'data cooperatives'[142] that would create a vast new ecosystem of minor intermediaries for data subjects to choose from. As a different way of organising the data economy, this would be, in principle, a preferable democratic alternative to the extant arrangement. However, in practical terms, this approach risks putting the cart before the horse, by acting as if the political, economic and infrastructural support for these decentralised intermediaries already existed. In fact, it does not: with private monopolies sucking all the oxygen out of the economy, there's no space for an ecosystem of smaller alternatives to blossom. At least, that is, without relying on the permission and largesse of profit-driven giants.

Under present market conditions – where competition is low and capital is hoarded by a few – it seems much more likely that start-ups for democratic data governance would either fizzle/fail or be acquired/crushed.



How to get from here to there

Alternative data governance proposals listed above represent novel and unexplored models that require better understanding and testing to demonstrate proof of concept. The success of these alternative data governance models will require (aside from a fundamental re-conceptualisation of market power and political, economic and infrastructural support; see more in the text box on 'Paving the way for a new ecosystem of decentralised intermediaries'), strong regulations and enforcement mechanisms, to ensure data is stewarded in the interests of their beneficiaries.

The role, responsibilities and standards of practice remain to be fully defined and should include aspects of:

- enforcing data rights and obligations (e.g. compliance with data protection legislation),
- achieving a level of maturity of expertise and competence in the administration of a data intermediary, especially if its mission requires it to negotiate with large companies
- establishing clear management decision-making around delegation and scrutiny, and setting out the overarching governance of the 'data steward', which could be a newly established professional role (a data trustee or capable managers and administrators in a data cooperative) or a governing board (for example formed by individuals that have shares in a cooperative based on the data contributed). The data contributed may define the role of an individual in the board and the decision-making power regarding data use.

Supportive regulatory conditions are needed, to ease the process of porting individual and collective data into alternative governance models, such as a cooperative. Today, it is a daunting – if not impossible – task to ask a person to move all their data over to a new body (data access requests can take a long time to be processed, and often the data received needs to be 'cleaned' and restructured in order to be used elsewhere).

Legal mechanisms and technical standards must evolve to make that process easier. Ideally, this would produce a process that cooperatives, trusts and data stewardship bodies could undertake on behalf of individuals (the service they provide could include collecting and pooling data; see below on the Data Governance Act). Data portability, as defined by the GDPR, is not sufficient as a legal basis because it covers only data provided by the data subject and relies heavily on individual agency, whereas in the current data ecosystem, the most valuable data is generated about individuals without their knowledge or control.

Alternative data governance models have already made their way into legislation. In particular, the recently adopted EU Data Governance Act (DGA) creates a framework for voluntary data sharing via data intermediation services, and a mechanism for sharing and pooling data for 'data altruism' purposes.[143] The DGA mentions a specific category of data intermediation services that could support data subjects in exercising their data rights under the GDPR, however this option is only briefly offered in one of the recitals as one of the options, and lacks detail as to the practical implementation.[144]

The DGA also emphasises the importance of neutral and independent data-sharing intermediaries and sets out the criteria for entities that want to provide data-sharing services (organisations that provide only data intermediation services, and companies that offer data intermediation services in addition to other services, such as data marketplaces).[145] One of the criteria is that service providers may not use the data for purposes other than to put it at the disposal of data users, and must separate its data intermediation services structurally from any other value-added services it may provide. At the same time, data intermediaries will bear fiduciary duties towards individuals, to ensure that they act in the best interests of the data holders.[146]

Today there is a basic legal framework for data portability under the GDPR, which has been complemented with new portability rules in legislation, such as in the DMA. More recently, a new framework has been adopted that encourages voluntary data sharing and defines the criteria and conditions for entities that want to serve as a data steward or data intermediary. What are still needed are the legal, technical and interoperability mechanisms for individuals as well as collectives to effectively reclaim their data (including behavioural observations and statistical patterns that not only convey real economic value but can also serve individual and collective empowerment) from private entities (either directly or via trusted intermediaries), and a set of safeguards protecting these individuals and collectives from being, once again, exploited by another powerful agent (i.e. making sure that a data intermediary will remain independent and trustworthy, and is able to perform their mandate effectively in the wider data landscape).

The risk of amplifying collective harm

Jef Ausloos, Alexandra Giannopoulou and Jill Toh

So-called 'data intermediaries' have been framed as one practical way through which the collective dimension of data rights could be given shape in practice.[147] While they show some promise for more effectively empowering people and curbing collective data harms,[148] their growing popularity in policy circles mainly stems from their assumed economic potential.

Indeed, the political discourse at EU level, particularly in relation to the Data Governance Act (DGA) focuses on the economic objectives of data intermediaries, framing them in terms of their supposedly 'facilitating role in the emergence of new data-driven ecosystems'.[149] People's rights, freedoms and interests are only considered to the extent that the data intermediaries empower *individual* data subjects.

This focus on the (questionable) economic potential of data intermediaries and *individual* empowerment of data subjects raises significant concerns. Without clear constraints on the type of actors that can perform the role of intermediaries, their model can easily be usurped by the interests of those with (economic and political) power, at the cost of both individual and collective rights, freedoms and interests. Even more, their legal entrenching in EU law, risks amplifying collective data-driven harms. Arguably, for 'data intermediaries' to positively contribute to curbing collective harm and constraining power asymmetries, it will be important to move beyond the dominant narrative focusing on the individual and economic potential. Clear legal and organisational support in exercising data rights in a coordinated manner are a vital step in this regard.

To begin charting out the role of data intermediaries in the digital landscape, there is a need to explore questions such as: What are the first steps towards building alternative forms of data governance? How to undermine the power of companies that now enclose and control the data lifecycle? What is the role of the public sector in reclaiming power over data? How to ensure legitimacy of new data governance institutions? The text below offers some food for thought by exploring these important questions.

Paving the way for a new ecosystem of decentralised intermediaries

Jathan Sadowski

Efforts to build alternative forms of data governance should focus on changing its political economic foundations. We should focus on advancing two related strategies for reform that would pave the way for a new ecosystem of decentralised intermediaries.

The first strategy is to disintermediate the digital economy by limiting private intermediaries' ability to enclose the data lifecycle – the different phases of data management, including construction, collection, storage, processing, analysis, use, sharing, maintenance, archiving and destruction.

The digital economy is currently hyper-intermediated. We tend to think of the handful of massive monopolistic platforms that have installed themselves as necessary middlemen in production, circulation, and consumption processes. But there is also an overabundance of smaller, yet powerful, companies that insert themselves into every technical, social and economic interaction to extract data and control access.

Disintermediation means investigating what kind of policy and regulatory tools can constrain and remove the vast majority of these intermediaries whose main purpose is to capture – often without creating – value.[150] For example, disintermediation would require clamping down on the expansive secondary market for data, such as the one for location data,[151] which incentivises many companies to engage in the collection and storage of all possible data, for the purposes of selling and sharing with, or servicing, third parties such as advertisers.

Even more fundamental reforms could target the rights of control and access that companies possess over data assets and networked devices, which are designed to shut out regulators and researchers, competitors and consumers from understanding, challenging and governing the power of intermediaries. Establishing such limits is necessary for governing the lifecycle of data, while also making space for different forms of intermediaries designed with different purposes in mind.

In a recent example, after many years of fighting against lobbying by technology companies, the US Federal Trade Commission has voted to enforce 'right to repair' rules that grant users the ability to fix and modify technologies like smartphones, home appliances and vehicles without going through repairs shops 'authorised' by the manufacturers. [152] This represents a crucial transference of rights away from intermediaries and to the public.

The second strategy consists of the construction of new public institutions for democratic governance of data.

Achieving radical change requires advocating for forms of large-scale intervention that actively aim to undermine the current conditions of centralised control by corporations. In addition to pushing to expand the enforcement of data rights and privacy protections, efforts should be directed at policies for reforming government procurement practices and expanding public capacities for data governance.

The political and financial resources already exist to create and fund democratic data intermediaries. But funds are currently directed at outsourcing government services to technology companies, rather than insourcing the development of capacities through new and existing institutions. Corporate executives have been happy to cash the cheques of public investment, and a few large companies have managed to gain a substantial hold on public administration procurement worldwide.

Ultimately, strong legal and institutional interventions are needed in order to foundationally transform the existing arrangements of data control and value. Don't think of alternative data intermediaries (such as public data trusts in the model advocated for in this article)[153] as an endpoint, but instead as the beginning for a new political economy of data – one that will allow and nurture the growth of more decentralised models of data stewardship.

Public data trusts would be well positioned to provide alternative decentralised forms of data intermediaries with the critical resources they need – e.g. digital infrastructure, expert managers, financial backing, regulatory protections and political support – to first be feasible and then to flourish. Only then can we go beyond rethinking and begin rebuilding a political economy of data that works for everybody.[154]

Food for thought

In order to trigger further discussion, a set of problems and questions, which arise around alternative data governance institutions and the role they can play in generating transformative power shifts, are offered as provocations:

1. **Alternative data governance models can play a role at multiple levels.** They can work both for members that have direct contributions (e.g. members pooling data in a data cooperative and being actively engaged in running the cooperative), as well as for indirect members (e.g. when the scope of a data cooperative is to have wider societal effects). This raises questions such as: How are 'beneficiaries' of data identified and determined? Who makes those determinations, and by what method?

2. **Given the challenges of the current landscape, there are questions about what is needed in order for data intermediaries to play an active and meaningful role that leads to responsible data use and management in practice.** What would it take for these new governance models to actually increase control around the ways data is used currently (e.g. to forbid certain data uses)? Would organisations have to be mandated to deal with such new structures or adhere to their wishes even for data not pooled inside the model?

3. **In practice, there can be multiple types of data governance structures, potentially with competing interests.** For example some of them could be set up to restrict and to protect data, while others could be set up to maximise income streams for members from data use. If potential income streams are dependent on the use of data, what are the implications for privacy and data protection? How can potential conflicts between data intermediaries be addressed and by whom? What kinds of incentives structures might arise and what type of legal underpinnings do these alternative data governance models need to function correctly?

4. **The role of the specific parties involved in managing data intermediaries, their responsibilities and qualifications need to be considered and balanced**. Under what decision-making and management models would these structures operate, and how are decisions being made in practice? If things go wrong, who is held responsible, and by what means?

5. **The particularities of different digital environments across the globe lead to questions of applicability in different jurisdictions**. Can these models be translated/work in different regions around the world, including the less developed?

What about Web3?

Some readers might ask why this report does not discuss 'Web3' technologies – a term coined by Gavin Wood in his 2014 essay, which envisions a reconfiguration of the web's technical, governance and payments/transactions infrastructure that moves away from 'entrusting our information to arbitrary entities on the internet'.[167]

The original vision of Web3 aimed to decentralise parts of the online web experience and remove middlemen and intermediaries. It proposed four core components for a Web 3.0 or a 'post-Snowden' web:

- **Content publication:** a decentralised, encrypted information publication system that ensures the downloaded information hasn't been interfered with. This system could be built using principles that have been previously used in technologies such as the Bittorrent[168] protocol for peer-to-peer content distribution and HTTPS for secure communication over a computer network.
- **Messaging:** a messaging system that ensures communication is encrypted and traceable information is not revealed (e.g. IP addresses).
- **Trustless transactions:** a means of agreeing the rules of interaction within a system and ensuring automatic enforcement of these rules. A consensus algorithm prevents powerful adversaries from derailing the system. Bitcoin is the most popular implementation of this technology and establishes a peer-to-peer system for validating transactions without a centralised authority. While blockchain technology is associated primarily with payment transactions, the emergence of smart contracts has extended the set of use cases to more complex financial arrangements and non-financial interactions such as voting, exchange, notarisation or providing evidence.
- **Integrated user interface:** a browser or user interface that provides a similar experience to traditional web browsers, but uses a different technology for name resolution. In today's internet, the domain name system (DNS) is controlled by the Internet Corporation of Assigned Names and Numbers (ICANN) and delegated registrars. This would be replaced by a decentralised, consensus-based system which allows users to navigate the internet pseudonymously, securely and trustlessly (an early example of this technology is Namecoin).

Most elements of this initial Web3 vision are still in their technological infancy. Projects that focus on decentralised storage (for example BitTorrent, Swarm, IPFS) and computation (e.g. Golem, Ocean) face important challenges on multiple fronts – performance, confidentiality, security, reliability, regulation – and it is doubtful that the current generation of these technologies are able to provide a long-term, feasible alternative to existing centralised solutions for most practical use cases.

Bitcoin and subsequent advances in blockchain technology have achieved wider adoption and considerably more media awareness, although the space has been rife with various forms of scams and alarming business practices, due to rapid technological progress and lagging regulatory intervention.

Growing interest in blockchain networks has also contributed to the 'Web3 vision' being gradually co-opted by venture capital investors, to promote a particular niche of projects. This has popularised Web3 as an umbrella term for alternative financial infrastructure – such as payments, collectibles (non-fungible tokens or NFTs) and decentralised finance (DeFi) – and encouraged an overly simplistic perception of decentralisation.[169] It is not often discussed nor widely acknowledged that the complex architecture of these systems can (and often does) lead to centralisation of power re-emerging in the operational, incentive, consensus, network and governance layers.[170]

The promise of Web3 is that decentralisation of infrastructure will necessarily lead to decentralisation of digital power. There is value in this argument and undoubtedly some decentralised technologies, after they reach a certain level of maturity and if used in the right context, can offer benefits over existing centralised alternatives.

Acknowledging the current culture and state of development around Web3, at this stage there are few examples in this space where values such as decentralisation and power redistribution are front and centre. It would be interesting to see whether progressive alternatives deliver on their promise in the near to medium terms and take these values to the core.

4. Ensuring public participation in technology policy making

The vision

This is a world in which everybody who wants to participate in decisions about data and its governance can do so – there are mechanisms for engagement to legitimate needs and expectations of those affected by technology. Through a broad range of participatory approaches – from citizens' councils and juries that directly inform local and national data policy and regulation, to public representation on technology company governance boards – people are better represented, more supported and empowered to make data systems and infrastructures work for them, and policymakers are better informed about what people expect and desire from data, technologies and their uses.

Through these mechanisms for participatory data and technology policymaking and stewardship, individuals who wish to be active citizens can participate directly in data governance and innovation, whereas those who want their interests to be better represented have mechanisms where their voices and needs are represented through members of their community or through organisations.

Policymakers are more empowered through the legitimacy of public voice to act to curb the power of large technology corporations, and equipped with credible evidence to underpin approaches to policy, regulation and governance.

Public participation, engagement and deliberation have emerged in recent years as fundamental components in shaping future approaches to regulation across a broad spectrum of policy domains.[155] However, despite their promising potential to facilitate more effective policymaking and regulation, the role of public participation in data and technology-related policy and practice remains remarkably underexplored, if compared – for example – to public participation in city planning and urban law.

There is, however, a growing body of research that aims to understand the theoretical and practical value of public participation approaches for governing the use of data, which is described in our 2021 report, *Participatory data stewardship*.[156]

What is public participation?

Public participation describes a wide range of methods that bring members of the public's voices, perspectives, experiences and representation to social and policy issues. From citizen panels to deliberative polls, surveys to community co-design, these methods have important benefits, including informing more effective and inclusive policymaking, increasing representation and accountability in decision making, and enabling more trustworthy governance and oversight.[157]

Participation often involves providing members of the public with information about particular uses of data or technology, including access to experts, and time and space to reflect and develop informed opinions. Different forms of public participation are often described on a spectrum from 'inform', 'consult' and 'involve', through to 'collaborate' and 'empower'.[158] In our report *Participatory Data Stewardship*, the Ada Lovelace Institute places this spectrum into the context of responsible data use and management.

How to get from here to there

Public participation, when implemented meaningfully and effectively, ensures that the values, experiences and perspectives of those affected by data-driven technologies are represented and accounted for in policy and practices related to those technologies.

This has multiple positive impacts. Firstly, it offers a more robust evidence base for developing technology policies and practices that meet the needs of people and society, by building a better understanding of people's lived experiences and helping to better align the development, deployment and oversight of technologies with societal values. Secondly, it provides policy and practice with greater legitimacy and accountability by ensuring those who are affected have their voices and perspectives taken into account.

Taken together, the evidence base and legitimacy offered by public participation can support a more responsible data and technology ecosystem that earns the trust of the public, rather than erodes and undermines it.

There is significant potential for public participation interventions to enable more innovative regulation and governance of data and the technologies built on it.

Possible approaches to this include:

1. Members of the public could be assigned by democratically representative random lottery to independent governance panels that provide oversight of dominant technology firms and public-interest alternatives. Those public representatives could be supported by a panel of civil society organisations that interact with governing boards and scrutinise the activity of different entities involved in data-driven decision-making processes.
2. Panels or juries of citizens could be coordinated by specialised civil society organisations to provide input on the audit and assessment of datasets and algorithms that have significant societal impacts and effects.[159]
3. Political institutions could conduct region-wide public deliberation exercises to gather public input and shape future regulation and enforcement of technology platforms. For example, a national or regional-wide public dialogue exercise could be conducted to consider how a novel technology application might be regulated, or to evaluate the implementation of different legislative proposals.
4. Participatory co-design or deliberative assemblies could be used to help articulate what public interest data and technology corporations might look like (see the 'BBC for Data', page 53 above), as alternatives to privatised and multinational companies.

These four suggestions represent just a selection of provocations, and are far from exhaustive. The outcomes of public participation and deliberation can vary, from high-level sets of principles on how data is used, to detailed recommendations that policymakers are expected to implement. But in order to be successful, such initiatives need political will, support and buy-in, to ensure that their outcomes are acknowledged and adopted. Without this, participatory initiatives run the risk of 'participation washing', whereby public involvement is merely tokenistic.

Additionally, it is important to note that public participation is not about shifting responsibility back to people and civil society to decide on intricate matters, or to provide the justifications or 'mandates' for uses of data and technology that haven't been ethically, legally or morally scrutinised. Rather it is about the institutions and organisations that develop, govern and regulate data and technology making sure they act in the best interests of the people who are affected by the use of data and technology.

Further considerations and provocative concepts

Marginalised communities in democratic governance

Jef Ausloos, Alexandra Giannopoulou and Jill Toh

As Europe and other parts of the world set out plans to regulate AI and other technology services, it is more urgent than ever to reflect critically on the value and practical application of those legally designed mechanisms in protecting social groups and individuals that are affected by high-risk AI systems and other technologies. The question of who has access to decision-making processes, and how these decisions are made, is crucial to address the harms caused by technologies.

The #BrusselsSoWhite conversations (a social media hashtag expounding on the lack of racial diversity in EU policy conversations)[160] have clearly shown the absence and lack of marginalised people in discussions around European technology policymaking,[161] despite the EU expressing its commitment to anti-racism and inclusion.[162]

Meaningful inclusion requires moving beyond the rhetoric, performativity and tokenisation of marginalised people. It requires looking inwards to assess if the existing work environment, internal practices, hiring and retention requirements are barriers to entry and exclusionary-by-design.[163] Additionally, mere representation is insufficient. This also requires a shift to recognise the value of different types of expertise, and seeing marginalised people's experiences and knowledge as legitimate, and equal.

There are a few essential considerations for achieving this.

Firstly, legislators and civil society – particularly those active in the field of 'technology law' – should consider a broader ambit of rights, freedoms and interests at stake in order to capture the appropriate social rights and collective values generally left out from market-driven logics. This ought to be done by actively engaging with the communities affected and interfacing more thoroughly with respective pre-existing legal frameworks and value systems.[164]

Secondly, the dominant narrative in EU techno-policymaking frames all considered fundamental rights and freedoms from the perspective of protecting 'the individual' against 'big tech'. This should be complemented with a wider concern for the substantial collective and societal harm generated and exacerbated by the development and use of data-driven technologies by private and public actors.

Thirdly, in consideration of the flurry of regulatory proposals, there should be more effective rules on lobbying, related to transparency and funding requirements and funding sources for thinktanks and other organisations. The revolving door between European institutions and technology companies continues to remain highly problematic and providing independent oversight with investigative powers is crucial.[165]

Lastly, more (law) is not always better. Especially, civil society and academia ought to think more creatively on how legal and non-legal approaches may prove to be productive in tackling the collective hams produced by (the actors controlling) data-driven technologies. Policymakers and enforcement agencies should proactively support such efforts.

Further to these considerations, one approach to embedding public participation into technology policymaking is to facilitate meaningful and diverse deliberation on the principles and values that should guide new legislation and inform technology design.

For example, to facilitate public deliberation on the rules governing how emerging technologies are developed, the governing institutions responsible for overseeing new technologies – be it local, national or supranational government – could establish a citizens' assembly.[166]

Citizens' assemblies can take various forms, from small groups of citizens in a local community discussing a single issue over a few days, to many hundreds of citizens from across regions considering a complex topic across a series of weeks and months.

Citizens' assemblies must include representation of a demographically diverse cross-section of people in the region. Those citizens should come together in a series of day-long workshops, hosted across a period of several months, and independently facilitated. During those workshops, the facilitators should provide objective and accessible information about the technological issue concerned and the objectives of legislative or technical frameworks.

The assembly must be able to hear from and ask questions to experts on the topic, representing a mix of independent professionals and those holding professional or official roles with associated parties – such as policymakers and technology developers.

At the end of their deliberations, the citizens in the assembly should be supported to develop a set of recommendations – free from influence of any vested parties – with the expectation that these recommendations will be directly addressed or considered in the design of any legislative or technical frameworks. Such citizens' assemblies can be an important tool, in addition to grassroot engagement in political parties and civil society, for bringing people into work on societal issues.

Food for thought

As policymakers around the world develop and implement novel data and technology regulations, it is essential that public participation forms a core part of this drafting process. At a time when trust in governments and technology companies is reaching record lows in many regions, policymakers must experiment with richer forms of public engagement beyond one-way consultations. By empowering members of the public to co-create the policy that impacts their lives, policymakers can create more representative and more legitimate laws and regulations around data.

In order to trigger further discussion, a set of questions are offered as provocations for thinking about how to implement public participation and deliberation mechanisms in practice:

1. **Public participation requires a mobilisation of resources and new processes throughout the cycle of technology policymaking**. What incentives, resources and support do policymakers and governments need, to be able to undertake public engagement and participation in the development of data and AI policy?

2. **Public participation methods need strategic design, and limits need to be taken into consideration.** Given the ubiquitous and multi-use nature of data and AI, what discrete topics and cases can be meaningfully engaged with and deliberated on by members of the public?

3. **Inclusive public participation is essential, to ensuring a representative public deliberation process that delivers outcomes for those affected by technology policymaking.** Which communities and groups are the most disproportionately harmed or affected by data and AI, and what mechanisms can ensure their experiences and voices are included in dialogue?

4. **It is important to make sure that public participation is not used as a 'stamp of approval' and does not become merely a tick-box exercise.** To avoid 'participation washing', what will encourage governments, industry and other power holders to engage meaningfully with the public, whereby recommendations made by citizens are honoured and addressed?

Conclusions and open questions

In this report, we started with two questions: What is a more ambitious vision for data use and regulation that can deliver a positive shift in the digital ecosystem? And what are the most promising interventions to create a more balanced system of power and a people-first approach for data?

In Chapter 1, we defined the central problem: that today's digital economy is built on deep-rooted exploitative and extractive data practices and forms of 'data rentiership,' which have resulted in the accrual of vast amounts of power to a handful of large platforms.

We explained how this power imbalance has prevented benefits to people, who are largely unable to control how their data is collected and used, and are increasingly disempowered from engaging in, seeking redress or contesting data-driven decisions that affect their lives.

In Chapter 2 we outlined four cross-cutting interventions concerning infrastructure, data governance, institutions and participation that can help redress that power imbalance in the current digital ecosystem. We recognise that these interventions are not sufficient to solve the problems described above, but we propose them as a realistic first step towards a systemic change.

From interventions, framed as objectives for policy and institutional change, we moved to provocative concepts: more tangible examples of how changing the power balance could work in practice. While we acknowledge that, in the current conditions, these concepts open up more questions than they give answers, we hope other researchers and civil society organisations will join us in an effort to build evidence that validates or establishes limitations to their usefulness.

Before we continue the exploration of specific solutions (legal rules, institutional arrangements, technical standards) that have the potential to transform the current digital ecosystem towards what we have called 'a people-first approach', we reiterate how important it is to think about this change in a systemic way.

A systemic vision envisages all four interventions as interconnected, mutually reinforcing and dependent on one another. And requires consideration of external 'preconditions' that could prevent or impede this systemic reform. We identify the preconditions for the interventions to deliver results as: the efficiency and values of the enforcement bodies, increasing the possibilities for individual and collective legal action, and reducing the dependency of key political stakeholders on (the infrastructure and expertise of) large technology companies.

In this last chapter we not only acknowledge political, legal and market conditions that determine the possibilities for transformation of the digital ecosystem, but also propose questions to guide further discussion about these – very practical – challenges:

1. Effective regulatory enforcement

Increased regulatory enforcement, in the context of both national and international cooperation, is a necessary precondition to the success of the interventions described above. As described in Chapter 1, resolving the regulatory enforcement problem will help create meaningful safeguards and regulatory guardrails to support change.

An important aspect of regulatory enforcement and cooperation measures includes the ability of one authority to supply timely information to other authorities from different sectors and from different jurisdictions, subject to relevant procedural safeguards. Some models of this kind of regulatory cooperation already exist – in the UK, the Digital Regulation Cooperation Forum (DRCF) is a cross-regulatory body formed in 2020 by the Competition and Markets Authority (CMA), and includes the Financial Conduct Authority (FCA), the Information Commissioner's Office (ICO) and the Office of Communications (Ofcom).[171]

Where regulatory action is initiated against major platforms and global players, new measures should be considered as part of international regulators' fora, that will provide the possibility to create ad hoc enforcement task forces across sectors and geographic jurisdictions, and to institutionalise such bodies, where necessary. The possibility of creating multi-sectoral and multi-geographic oversight and enforcement bodies focusing only on the biggest players in the global data and digital economy should be actively considered.

Moreover, it is necessary to create formal channels of communication between enforcement bodies, to be able to share sensitive information that might be needed in investigations. Currently, many enforcement authorities cannot share important information they have obtained in the course of their procedures with enforcement authorities that have a different area of competence or operate in a different jurisdiction. As data and all-purpose technologies are currently used by large platforms, any single enforcement body will not be able to see the full picture of risks and harms, leading to suboptimal enforcement of platforms and data practices. Coherent and holistic enforcement is needed.

Questions that need to be addressed:

- What would an integrated approach to regulation and enforcement be constituted in practice, embedding data protection, consumer protection and competition law objectives and mechanisms?
- How can we uphold procedural rights, such as the right to good administration and to effective judicial remedy, in the context of transnational and trans-sectoral disputes?
- How can enforcement authorities be made accountable where they fail to enforce the law effectively?
- How to build more resilient enforcement structures that are less susceptible to corporate capture?

Taking into account collective harm

Jef Ausloos, Alexandra Giannopoulou and Jill Toh

Despite efforts to prevent it from being a mere checkbox exercise, GDPR compliance efforts often suffer from a narrow-focused framing, ignoring the multifarious issues that (can) arise in complex data-driven technologies and infrastructures. A meaningful appreciation of the broader context and the evaluation of potential impacts on (groups of) individuals and communities is necessary in order to move from 'compliance' narratives to fairer data ecosystems that are continuously evaluated and confronted with the potential individual or collective harms caused by data-driven technologies.

Public decision-makers responsible for deploying new technologies should start by questioning critically the very reason for adopting a specific data-driven technology in the first place. These actors should fundamentally be able to first demonstrate the necessity of the system itself, before assessing what data collection and processing the respective system would require. For instance, in the example of the migrant-monitoring system Centaur used in new refugee camps in Greece, authorities should be able to first demonstrate in general terms the necessity of a surveillance system, before assessing the inherent data collection and processing that Centaur would require and what would justify as necessary.

This deliberation is a complex exercise. Where the GDPR requires a data protection impact assessment, this deliberation is left to data controllers, before being subject to any type of questioning by relevant authorities.

One problem is that data controllers often define the legitimacy of a chosen system by stretching the meaning of GDPR criteria, or by benefitting from the lack of strict compliance processes for principles (such as data minimisation and data protection by design and by default) in order to demonstrate compliance. This can lead to a narrow norm-setting environment, because even if operating under rather flexible concepts (such as the respect of data protection principles as set out in the GDPR), the data controllers' interpretation remains constricted in practice and neglects to consider new types of harms and impacts on a wider level.

While the responsibility to identify and mitigate harms is the responsibility of the data controller, civil society organisations could play an important facilitator role (without placing any formal burden to facilitate this process) in revealing collective harms that complex data-driven technological systems are likely to inflict on specific communities and groups, as well as sector-specific or community-specific interpretations of these harms.[172]

In practice, accountability measures would then require that the responsible actors need not only demonstrate the consideration of these possible broader collective harms, but also the active measures and steps taken to prevent them from materialising.

Put briefly, both data protection authorities and those controlling impactful data-driven technologies, need to recognise they can be held accountable for, and have to address, complex harms and impacts on individuals and communities. For instance, from a legal perspective, and as recognised under the GDPR's data protection by design and by default requirement,[173] this means that compliance ought not to be seen as a one-off effort at the start of any complex data-driven technological system, but rather a continuous exercise considering the broader implications of data infrastructures on everyone involved.

Perhaps more importantly, and because not all harms and impacts can be anticipated, robust mechanisms should be in place enabling and empowering affected individuals and communities to challenge (specific parts of) data-driven technologies. While the GDPR may offer some tools for empowering those affected (e.g. data rights), they cannot be seen as goals in themselves, but need to be interpreted and accommodated in light of the context in which, and interests for which, they are invoked.

2. Legal action and representation

Another way to support the proposed interventions in Chapter 2 having their desired effect is to create more avenues for civil society organisations, groups and individuals to hold large platforms accountable for abuses of their data rights, as well as state authorities that do not adequately fulfil their enforcement tasks.

Mandating the exercise of data rights to intermediary entities is being explored as a way to address information and power asymmetries and systemic data-driven injustices at a collective level. [174] The GDPR does not prevent the exercise of data rights through intermediaries, and rights delegation (as opposed to waiving the right to data protection, which is not possible under EU law since fundamental rights are inalienable), has started to be recognised in data protection legislation globally.

For example, in India[175] and Canada,[176] draft data protection and privacy bills speak about intermediaries that can exercise the rights conferred by law. In the US, the California Consumer Privacy Act (CCPA)[177] and the California Privacy Rights Act (CPRA)[178] – which amends and expands the CCPA – both mention 'authorised agents', and the South Korean Personal Information Protection Act [179] also talks about 'representatives' who can be authorised by the data subject to exercise rights.

Other legal tools enabling legal action for individuals and collectives are Article 79 of the GDPR, which allows data subjects to bring compliance orders before courts, and Article 80(2) of the GDPR, which allows representative bodies to bring collective actions without the explicit mandate of data subjects. Both these mechanisms are underused and underenforced, receiving little court attention.

One step further would be to strengthen the capacity for civil society to pursue collective legal action for rights violations directly against the large players or against state authorities that do not adequately fulfil their enforcement tasks. The effort of reforming legal action and representation rules in order to make them more accessible for civil society actors and collectives needs to include measures to reduce the high costs for bringing court claims.[180] Potential solutions could be cost-capping for certain general actions when the claimant cannot afford the case.

Questions that need to be addressed:

- How can existing mechanisms for legal action and representation be made more accessible to civil society actors and collectives?
- What new mechanisms and processes need to be designed for documenting abuses and proving harms, to address systemic data-driven injustices at a collective level?
- How can cost barriers to legal action be reduced?

3. Removing industry dependencies

Finally, another way to ensure the interventions described above are successful is to lessen dependencies between regulators, civil society organisations and corporate actors. Industry dependencies can take many forms, including the sponsoring of major conferences for academia and civil society, and funding policy-oriented thinktanks that seek to advise regulators.[181] [182] While these dependencies do not necessarily lead to direct influence over research outputs or decisions, they do raise a risk of eroding independent critique and evaluation of large digital platforms.

There are only a small number of specialist university faculties and research institutes working on data, digital and societal impacts that do not operate, in one way or another, with funding from large platforms.[183] This industry-resource dependency can risk jeopardising academic independence. A recent report highlighted that '[b]ig tech's control over AI resources made universities and other institutions dependent on these companies, creating a web of conflicted relationships that threaten academic freedom and our ability to understand and regulate these corporate technologies.'[184]

This points to the need for a more systematic approach to countering corporate dependencies. Civil society, academia and the media play an important role in counterbalancing the narratives and actions of large corporations. Appropriate public funding, statutory rights and protection are necessary for them to be able to fulfil their function as balancing actors, but also as visionaries for alternative and potentially better ecosystems.

Questions that need to be addressed:

- What would alternative funding models (such as public or philanthropic) that remove dependencies on industry be constituted?
- Could national research councils (such as UKRI) and public funding play a bigger role in creating dedicated funding streams to support universities, independent media and civil society organisations, to shield them from corporate financing?
- What type of mechanisms and legal measures need to be put in place, to establish endowment funds for specific purposes, creating sufficient incentives for founding members, but without compromising governance? (For example, donors, including large companies, could benefit from specific tax deductions but wouldn't have any rights or decision-making power in how an endowment is governed, and capital endowments would be allowed but not recurring operating support, as that creates dependency).

Open invitation and call to action

A complete overturn of the existing data ecosystem cannot happen overnight. In this report, we acknowledge that a multifaceted approach is necessary for such a reform to be effective. Needless to say, there is no single, off-the-shelf solution that – on its own – will change the paradigm. Looking towards ideas that can produce substantial transformations can seem overwhelming, and it is also necessary to acknowledge and factor in the challenges that lie with adopting less revolutionary ideas into practice.

Acknowledging that there are many instruments that remain to be fully tested and understood in existing legislation, in this report we set off to develop the most promising tools for intervention that can take us towards a people-first digital ecosystem that's fit for the middle of the twenty-first century.

In this intellectual journey, we explored a set of instruments, which carry transformative potential, and divided them into four areas that reflect the biggest obstacles we will face when imagining a deep reform of the digital ecosystem: control over technology infrastructure, power over how data is purposed and governed, balancing asymmetries with new institutions and more social accountability with inclusive participation in policymaking.

We unpacked some of the complexity of these challenges, and asked questions that we deem critical for the success of this complex reform. With this opening, we hope to fuel a collective effort to articulate ambitious aspirations for data use and regulation that work for people and society.

Reinforcing our invitation in 2020 to 'rethink data', we call on policymakers, researchers, civil society organisations, funders and industry to build towards more radical transformations, reflecting critically, testing and further developing these proposed concepts for change.

Who	What you can do
Policymakers	• Transpose the proposed interventions into policy action and help build the pathway towards a comprehensive and transformative vision for data. • Ensure that impediments to effective enforcement of existing regulatory regimes are identified and removed. • Use evidence of public opinion to proactively develop policy, governance and regulatory mechanisms that work for people and society.
Researchers	• Reflect critically on the goals, strengths and weaknesses of the proposed concepts for change. • Build on the proposed concepts for change with further research into potential solutions.
Civil society organisations	• Analyse the proposed transformations and propose ways to build a proactive (instead of reactive) agenda in policy. • Be ambitious and bold, visualise a positive future for data and society. • Advocate for transformative changes in data policy and practice and make novel approaches possible.
Funders	• Include exploration of the four proposed interventions in your annual funding agenda, or create a new funding stream for a more radical vision for data. • Support researchers and civil society organisations to remain independent of government and industry. • Fund efforts that work towards advancing concepts for systemic change.
Industry	• Support the development and implementation of open standards in a more inclusive way (incorporating diverse perspectives). • Contribute to developing mechanisms for the responsible use of data for social benefit. • Incorporate transparency into practices, including being open about internal processes and insights, and allowing researcher access and independent oversight.

Final notes

Context for our work

One of the core conundrums that motivated the establishment of the Ada Lovelace Institute by the Nuffield Foundation in 2018 was how to construct a system for data use and governance that engendered public trust, enabled the protection of individual rights and facilitated the use of data as a public good.

Even before the Ada Lovelace Institute was fully operational, Ada's originating Board members (Sir Alan Wilson, Hetan Shah, Professor Helen Margetts, Azeem Azhar, Alix Dunn and Professor Huw Price) had begun work on a prospectus to establish a programme of work, guided by a working group, to look 'beyond data ownership' at future possibilities for overhauling data use and management. This programme built on the foundations of the Royal Society and British Academy 2017 report, *Data Use and Management*, and grew to become Rethinking Data.

Ada set out an ambitious vision for a research programme, to develop a countervailing vision for data, which could make the case for its social value, tackle asymmetries of power and data injustice, and promote and enable responsible and trustworthy use of data. Rethinking Data aimed to examine and reframe the kinds of language and narratives we use when talking about data, define what 'good' looks like in practice when data is collected, shared and used, and recommend changes in regulations so that data rights can be effectively exercised, and data responsibilities are clear.

There has been some progress in changing narratives, practices and regulations: popular culture (in the form of documentaries such as *The Social Dilemma and Coded Bias*), corporate product choices (like Apple's decision to restrict tracking by default on iPhone apps) and high-profile news stories (such as the Ofqual algorithm fiasco, which saw students take to British streets to protest 'F**k the algorithm'), have contributed to an evolving and more informed narrative about data.

The potential of data-driven technologies has been front and centre in public health messaging around the pandemic response, and debates around contact tracing apps have revealed a rich and nuanced spectrum of public attitudes to the trade-off between individual privacy and the public interest. The Ada Lovelace Institute's own public deliberation research during the pandemic showed that the 'privacy vs the pandemic' arguments entrenched in media and policy narratives are contested by the public.[185]

There is now an emerging discourse around 'data stewardship', the responsible and trustworthy management of data in practice, to which the Ada Lovelace Institute has contributed via research which canvasses nascent legal mechanisms and participatory approaches for improving ethical data practices. [186] The prospect of new institutions and mechanisms for empowering individuals in the governance of their data is gaining ground, and the role of new data intermediaries is being explored in legislative debates in Europe, India and Canada, [187] as well as in the data reform consultation in the UK.[188]

Methodology

The underlying research for this project was primarily informed by the range of expert perspectives in the Rethinking data working group. It was supplemented by established and emerging research in this landscape and refined by several research pieces commissioned from leading experts on data policy.

Like most other things, the COVID-19 pandemic made the task of the Rethinking data working group immensely more difficult, not least because we had envisaged the deliberation of the group (which spans three continents) would take place in person. Despite this, the working group persisted and managed 10 meetings over a 12 month period.

To start with, the working group met to identify and analyse themes and tensions in the current data ecosystem. In the first stage of these deliberations, they singled out the key questions and challenges they felt were most important, such as questions around the infrastructure used to collect and store data, emerging regulatory proposals for markets and data-driven technologies, and the market landscape that major technology companies operate in.

Once these challenges were identified, the working group used a horizon-scanning methodology, to explore the underlying assumptions, power dynamics and tensions. To complement the key insights from the working group discussion, a landscape overview on 'future technologies' – such as privacy-enhancing techniques, edge computing, and others – was commissioned from the University of Cambridge.

The brief looked at emerging trends that present more pervasive, targeted or potentially intrusive data capture, focusing only on the more notable or growing models. The aim was to identify potential glimpses into how power will operate in new settings created by technology, and how the big business players' approach to people and data might evolve as a result of these new developments, without the intention to predict or to forecast how trends will play out.

Having identified power and centralisation of large technology companies as two of the major themes for concern, in the second stage of the deliberations, the two major questions the working group considered were: What are the most important manifestations of power? And what are the most promising interventions to enabling an ambitious vision for the future of data use and regulation?

Speculative thinking methodologies, such as speculative scenarios, were used as provocations for the working group, to think beyond the current challenges, allowing different concepts for interventions to be discussed. The three developed scenarios highlighted potential tensions and warned about fallacies that could emerge if a simplistic view around regulation was employed.

In the last stage of our process, the interventions suggested by the working group were mapped into an ecosystem of interventions that could support positive transformations to emerge. Commissioned experts were invited to surface further challenges, problems and open questions associated with different interventions.

Acknowledgements

This report was lead authored by Valentina Pavel, with substantive contributions from Carly Kind, Andrew Strait, Imogen Parker, Octavia Reeve, Aidan Peppin, Katarzyna Szymielewicz, Michael Veale, Raegan MacDonald, Orla Lynskey and Paul Nemitz.

Working group members

Diane Coyle (co-chair)
Bennett Professor of Public Policy, University of Cambridge

Paul Nemitz (co-chair)
Principal Adviser on Justice Policy, EU Commission, visiting Professor of Law at College of Europe

Amba Kak
Executive Director
AI Now Institute

Amelia Andersdotter
Data Protection Technical Expert and Founder, Dataskydd

Anne Cheung
Professor of Law, University of Hong Kong

Martin Tisné
Managing Director, Luminate

Michael Veale
Associate Professor of Law
University College London

Natalie Hyacinth
Senior Research Associate, University of Bristol

Natasha McCarthy
Head of Policy, Data, The Royal Society

Katarzyna Szymielewicz
President, Panoptykon Foundation

Orla Lynskey
Associate Professor of Law, London School of Economics

Raegan MacDonald
Tech-policy expert

Rashida Richardson
Assistant Professor of Law and Political Science, Northeastern University School of Law & College of Social Sciences and Humanities

Ravi Naik
Legal Director, AWO

Steven Croft
Founding board member, Centre for Data Ethics and Innovation (CDEI)

Taylor Owen
Associate Professor, McGill University – Max Bell School of Public Policy

Commissioned experts

Ian Brown
Leading specialist on internet regulation and pro-competition mechanisms such as interoperability

Jathan Sadowski
Senior research fellow, Emerging Technologies Research Lab, Monash University

Jef Ausloos
Institute for Information Law (IViR), University of Amsterdam

Jill Toh
Institute for Information Law (IViR), University of Amsterdam

Alexandra Giannopoulou
Institute for Information Law (IViR), University of Amsterdam

External reviewers

Agustín Reyna
Director, Legal and Economic Affairs
BEUC

Alek Tarkowski
Director of Strategy
Open Future Foundation

Jeni Tennison
Executive Director, Connected by data

Theresa Stadler
Doctoral assistant, Security and Privacy Engineering Lab, at Ecole Polytechnique Fédérale de Lausanne (EPFL)

Throughout the working group deliberations we also received support from Annabel Manley, research assistant at the University of Cambridge, and Jovan Powar and Dr Jat Singh, Compliant & Accountable Systems Group at the University of Cambridge.

About the Ada Lovelace Institute

The Ada Lovelace Institute was established by the Nuffield Foundation in early 2018, in collaboration with the Alan Turing Institute, the Royal Society, the British Academy, the Royal Statistical Society, the Wellcome Trust, Luminate, techUK and the Nuffield Council on Bioethics.

The mission of the Ada Lovelace Institute is to ensure that data and AI work for people and society. We believe that a world where data and AI work for people and society is a world in which the opportunities, benefits and privileges generated by data and AI are justly and equitably distributed and experienced.

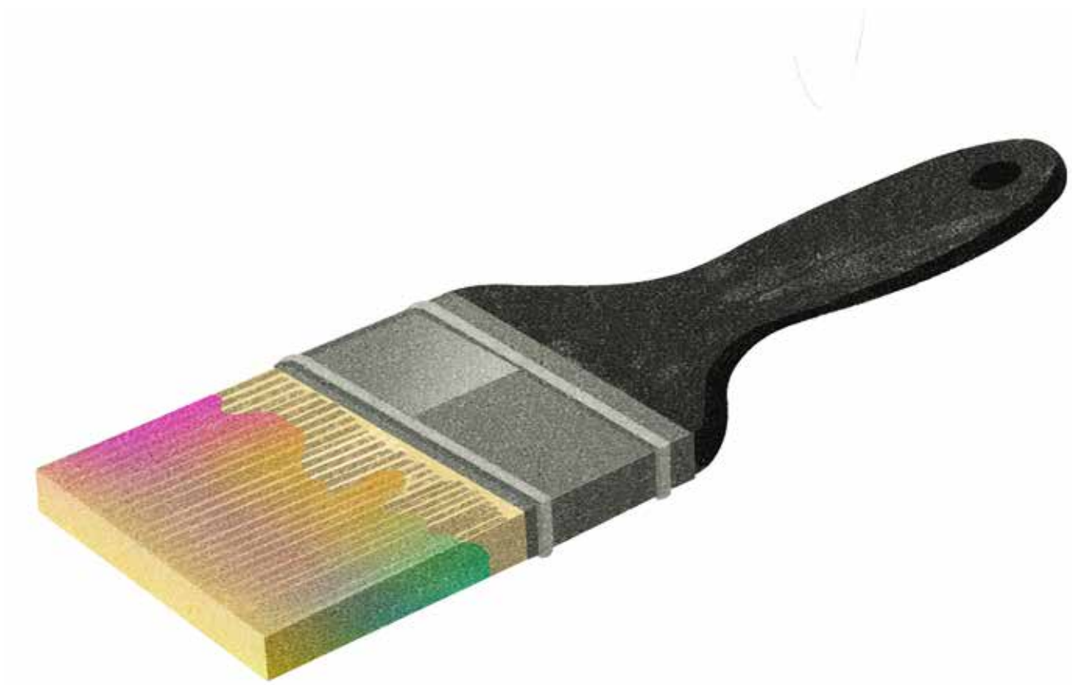
We recognise the power asymmetries that exist in ethical and legal debates around the development of data-driven technologies, and will represent people in those conversations. We focus not on the types of technologies we want to build, but on the types of societies we want to build.

Through research, policy and practice, we aim to ensure that the transformative power of data and AI is used and harnessed in ways that maximise social wellbeing and put technology at the service of humanity.

We are funded by the Nuffield Foundation, an independent charitable trust with a mission to advance social wellbeing. The Foundation funds research that informs social policy, primarily in education, welfare and justice. It also provides opportunities for young people to develop skills and confidence in STEM and research. In addition to the Ada Lovelace Institute, the Foundation is also the founder and co-funder of the Nuffield Council on Bioethics and the Nuffield Family Justice Observatory

Find out more

Website: adalovelaceinstitute.org
Twitter: @AdaLovelaceInst
Email: hello@adalovelaceinstitute.org



End notes

1 Ada Lovelace Institute. (2020). *Rethinking Data– Prospectus*. Available at: https://www.adalovelaceinstitute.org/wp-content/uploads/2020/01/Rethinking-Data-Prospectus-Ada-Lovelace-Institute-January-2019.pdf

2 Ada Lovelace Institute. (2020). *The data will see you now*. Available at: https://www.adalovelaceinstitute.org/report/the-data-will-see-you-now/

3 Statista Research Department. (2022). *Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025*. Available at: https://www.statista.com/statistics/871513/worldwide-data-created/

4 Balayn, A. and Gürses, S. (2021). *Beyond Debiasing, Regulating AI and its inequalities*. European Digital Rights (EDRi). Available at: https://edri.org/wp-content/uploads/2021/09/EDRi_Beyond-Debiasing-Report_Online.pdf

5 Zuboff, S. (2019). *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. New York: PublicAffairs and Cohen, J. E. (2019). *Between truth and power: the legal constructions of informational capitalism*. New York: Oxford University Press.

6 Birch, K., Chiappetta, M. and Artyushina, A. (2020). 'The problem of innovation in technoscientific capitalism: data rentiership and the policy implications of turning personal digital data into a private asset'. *Policy Studies*, 41(5), pp. 468–487. doi: 10.1080/01442872.2020.1748264

7 Hwang, T. (2020). *Subprime attention crisis: advertising and the time bomb at the heart of the Internet*. New York: FSG Originals.

8 Fitzgerald M. and Crider C. (2020). 'Under pressure, UK government releases NHS COVID data deals with big tech'. openDemocracy. Available at: https://www.opendemocracy.net/en/ournhs/under-pressure-uk-government-releases-nhs-covid-data-deals-big-tech/

9 European Commission – Expert Group for the Observatory on the Online Platform Economy. (2021). *Uncovering blindspots in the policy debate on platform power*. Available at: https://www.sipotra.it/wp-content/uploads/2021/03/Uncovering-blindspots-in-the-policy-debate-on-platform-power.pdf

10 European Commission – Expert Group for the Observatory on the Online Platform Economy. (2021).

11 Cohen, J.E. (2019). *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford: Oxford University Press.

12 Andersdotter, A. and Stasi, I. *Framework for studying technologies, competition and human rights*. Available at: https://amelia.andersdotter.cc/framework_for_competition_technology_and_human_rights.html

13 Cohen, J. E. (2017). 'Law for the Platform Economy'. *U.C. Davis Law Review*, 51, pp. 133–204. Available at: https://perma.cc/AW7P-EVLC

14 Mozur, P., Kang, C., Satariano, A. and McCabe, D. (2021). 'A Global Tipping Point for Reining In Tech Has Arrived'. *New York Times*. Available at: https://www.nytimes.com/2021/04/20/technology/global-tipping-point-tech.html

15 Australia's Online Safety Act (2021). Available at: https://www.legislation.gov.au/Details/C2021A00076

16 Ministry of Electronics and Information Technology. (2021). *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*. Available at: https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021

17 European Parliament. (2022). *Legislative resolution of 5 July 2022 on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act)*. Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0269_EN.html

18 *Online Safety Bill*. (2022-23). Parliament: House of Commons. Bill no. 121. London: Published by the authority of the House of Commons. Available at https://bills.parliament.uk/bills/3137

19 While statutory legislation will not be introduced in the 2022–23 Parliamentary session, the UK Government reconfirmed its intention to establish the Digital Market Unit's statutory regime in legislation as soon as Parliamentary time allows. See: Hayter, W. (2022). 'Digital markets and the new pro-competition regime'. *Competition and Markets Authority*. Available at: https://competitionandmarkets.blog.gov.uk/2022/05/10/digital-markets-and-the-new-pro-competition-regime/ and UK Government. (2021). 'Digital Markets Unit'. *Gov.uk*. Available at https://www.gov.uk/government/collections/digital-markets-unit

20 European Parliament and Council of the European Union. (2022). *Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)*, Article 5(2) and Article 6(5). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A265%3ATOC

21 Ansari, A. A. (2022), 'E-commerce is the latest target in India's push for an open digital economy'. *Atlantic Council*. Available at: https://www.atlanticcouncil.org/blogs/southasiasource/e-commerce-is-the-latest-target-in-indias-push-for-an-open-digital-economy/

22 Aryan, A., Pinnu, S. and Agarwal, S. (2022). 'Govt looks to table data bill soon, draft at advanced stage'. *Economic Times*. Available at: https://telecom.economictimes.indiatimes.com/news/govt-looks-to-table-data-bill-soon-draft-at-advanced-stage/93358857 and Raj, R. (2022). 'Data protection: Four key clauses may go in new bill'. *Financial Express*. Available at: https://www.financialexpress.com/industry/technology/data-protection-four-key-clauses-may-go-in-new-bill/2618148/

23 Greenleaf, G. (2021). 'Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance'. *Privacy Laws & Business International Report*, 1, pp. 3–5.

24 Corporate Europe Observatory. (2021). *The Lobby Network: Big Tech's Web of Influence in the EU*. Available at: https://corporateeurope.org/en/2021/08/lobby-network-big-techs-web-influence-eu

25 Rich, J. (2021). 'After 20 years of debate, it's time for Congress to finally pass a baseline privacy law'. Brookings. Available at https://www.brookings.edu/blog/techtank/2021/01/14/after-20-years-of-debate-its-time-for-congress-to-finally-pass-a-baseline-privacy-law/ and Levine, A. S. (2021). 'A U.S. privacy law seemed possible this Congress. Now, prospects are fading fast'. *Politico*. Available at: https://www.politico.com/news/2021/06/01/washington-plan-protect-american-data-silicon-valley-491405

26 Zanfir-Fortuna, G. (2020). 'America's "privacy renaissance": What to expect under a new presidency and Congress'. *Ada Lovelace Institute*. Available at https://www.adalovelaceinstitute.org/blog/americas-privacy-renaissance/

27 American Data Privacy and Protection Act, discussion draft, 117th Cong. (2021). Available at: https://www.commerce.senate.gov/services/files/6CB3B500-3DB4-4FCC-BB15-9E6A52738B6C

28 Hoofnagle, C. J., Hartzog, W. and Solove, D. J. (2019). 'The FTC can rise to the privacy challenge, but not without help from Congress'. *Brookings*. Available at: https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/

29 Bietti, E. (2021). 'Is the goal of antitrust enforcement a competitive digital economy or a different digital ecosystem?'. *Ada Lovelace Institute*. Available at: https://www.adalovelaceinstitute.org/blog/antitrust-enforcement-competitive-digital-economy-digital-ecosystem/

30 House Judiciary Committee's Antitrust Subcommittee. (2020). *Investigation of Competition in the Digital Marketplace: Majority Staff Report and Recommendations*. Available at: https://judiciary.house.gov/news/documentsingle.aspx?DocumentID=3429

31 In the case of Facebook, see the Federal Trade Commission and the State Advocate General cases: https://www.ftc.gov/enforcement/cases-proceedings/191-0134/facebook-inc-ftc-v and https://ag.ny.gov/sites/default/files/facebook_complaint_12.9.2020.pdf. In the case of Google, see the Department of Justice and the State Advocate General cases: https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws and https://coag.gov/app/uploads/2020/12/Colorado-et-al.-v.-Google-PUBLIC-REDACTED-Complaint.pdf

32 Ada Lovelace Institute. (2021). 'Ada Lovelace Institute hosts "Taking back control of data: scrutinising the UK's plan to reform the GDPR"'. Available at: https://www.adalovelaceinstitute.org/news/data-uk-reform-gdpr/

33 See: UK Government. (2021). *National AI Strategy*. Available at: https://www.gov.uk/government/publications/national-ai-strategy and UK Government. (2020). National Data Strategy. Available at: https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy

34 UK Government. (2022). *Data: a new direction – Government response to consultation*. Available at: https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation

35 *Data Protection and Digital Information Bill*. (2022-23). Parliament: House of Commons. Bill no. 143. London: Published by the authority of the House of Commons. Available at: https://bills.parliament.uk/bills/3322/publications

36 Stanford University. (2021). *Artificial Intelligence Index 2021*, chapter 7. Available at https://aiindex.stanford.edu/wp-content/uploads/2021/03/2021-AI-Index-Report-_Chapter-7.pdf and OECD/European Commission. (2021). *AI Policy Observatory*. Available at: https://oecd.ai/en/dashboard

37 Ministério da Ciência, Tecnologia e Inovações. (2021). *Estratégia Brasileira de Inteligência Artificial*. Available at: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/inteligencia-artificial

38 See: National Artificial Intelligence Initiative Act, 116th Cong. (2020). Available at https://www.congress.gov/bill/116th-congress/house-bill/6216 and the establishment of the National Artificial Intelligence Research Resource Task Force: The White House. (2021). 'The Biden Administration Launches the National Artificial Intelligence Research Resource Task Force'. Available at: https://www.whitehouse.gov/ostp/news-updates/2021/06/10/the-biden-administration-launches-the-national-artificial-intelligence-research-resource-task-force/

39 UK Government. (2021). *National AI Strategy*. Available at: https://www.gov.uk/government/publications/national-ai-strategy

40 For concerns raised by the US National Artificial Intelligence Research Resource (NAIRR) see: AI Now and Data & Society's joint comment. Available at https://ainowinstitute.org/AINow-DS-NAIRR-comment.pdf

41 For a detailed analysis, see: Dorwart, H., Zanfir-Fortuna, G. and Girot, C. (2021). 'China's New Comprehensive Data Protection Law: Context, Stated Objectives, Key Provisions'. *Future of Privacy Forum*. Available at https://fpf.org/blog/chinas-new-comprehensive-data-protection-law-context-stated-objectives-key-provisions/

42 Creemers, R. (2021). 'China's Emerging Data Protection Framework'. *Social Science Research Network*. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3964684

43 Creemers, R. (2021).

44 Owen, T. (2020). 'Doctorow versus Zuboff'. *Centre for International Governance Innovation*. Available at https://www.cigionline.org/articles/doctorow-versus-zuboff/

45 European Parliament and Council of the European Union. (2022). *Digital Markets Act*, Article 7, Article 6 and Recital 57. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A265%3ATOC

46 European Parliament and Council of the European Union. (2022). Article 6 (10).

47 European Parliament and Council of the European Union. (2022). *Digital Markets Act*, Article 6 (9). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A265%3ATOC

48 European Parliament and Council of the European Union. (2022). *Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868&qid=1657887017015

49 European Commission. (2021). *Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act)*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN

50 European Commission. (2021). *Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

51 Ryan, J. and Toner, A. (2020). 'Europe's governments are failing the GDPR'. *brave.com*. Available at: https://brave.com/static-assets/files/Brave-2020-DPA-Report.pdf and European Data Protection Board (2020). *Contribution of the EDPB to the evaluation of the GDPR under Article 97*. Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf

52 More details at Irish Council for Civil Liberties. See: https://www.iccl.ie/rtb-june-2021/

53 Irish Council for Civil Liberties. (2018). *Regulatory complaint concerning massive, web-wide data breach by Google and other 'ad tech' companies under Europe's GDPR*. Available at: https://www.iccl.ie/digital-data/regulatorycomplaint-concerning-massive-web-wide-data-breach-by-google-and-other-ad-tech-companies-undereuropes-gdpr/

54 See: Irish Council for Civil Liberties. (2022). 'ICCL sues DPC over failure to act on massive Google data breach'. Available at https://www.iccl.ie/news/iccl-sues-dpc-over-failure-to-act-on-massive-google-data-breach/; Irish Council for Civil Liberties. (2021). 'ICCL lawsuit takes aim at Google, Facebook, Amazon, Twitter and the entire online advertising industry'. Available at https://www.iccl.ie/news/press-announcement-rtb-lawsuit/; and Open Rights Group. *Ending illegal online advertising*. Available at: https://www.openrightsgroup.org/campaign/ending-adtech-abuse/

55 Belgian Data Protection Authority. (2022). 'The BE DPA to restore order to the online advertising industry: IAB Europe held responsible for a mechanism that infringes the GDPR'. Available at: https://www.dataprotectionauthority.be/citizen/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr

56 Data Protection Commission. (2021). 'Data Protection Commission announces decision in WhatsApp inquiry'. Available at: https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry

57 The European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) also issued a draft motion in 2021 in relation to how the Irish DPC was handling the 'Schrems II' case and recommended the European Commission to start the infringement procedures against Ireland for not properly enforcing the GDPR.

58 Espinoza, J. (2021). 'Fighting in Brussels bogs down plans to regulate Big Tech'. *Financial Times*.. Available at: https://www.ft.com/content/7e8391c1-329e-4944-98a4-b72c4e6428d0

59 Manancourt, V. (2021). 'EU privacy law's chief architect calls for its overhaul'. *Politico*. Available at: https://www.politico.eu/article/eu-privacy-laws-chief-architect-calls-for-its-overhaul/

60 Burgess, M. (2020). 'MPs slam UK data regulator for failing to protect people's rights'. *Wired UK*. Available at: https://www.wired.co.uk/article/ico-data-protection-gdpr-enforcement; Open Rights Group (2021). 'Open Rights Group calls on the ICO to do its job and enforce the law'. Available at: https://www.openrightsgroup.org/press-releases/open-rights-group-calls-on-the-ico-to-do-its-job-and-enforce-the-law/

61 Erdos, D. (2020). 'Accountability and the UK Data Protection Authority: From Cause for Data Subject Complaint to a Model for Europe?'. *Social Science Research Network*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3521372

62 Lynskey, O. (2021). 'EU-UK Data Flows: Does the "New Direction" lead to "Essentially Equivalent" Protection?'. *The Brexit Institute*. Available at https://dcubrexitinstitute.eu/2021/09/eu-uk-data-new-direction/

63 Erdos, D. (2022). 'What Way Forward on Information Rights Regulation? The UK Information Commissioner's Office Launches a Major Consultation'. *Inforrm*. Available at https://inforrm.org/2022/01/21/what-way-forward-on-information-rights-regulation-the-uk-information-commissioners-office-launches-a-major-consultation-david-erdos/

64 Delli Santi, M. (2022). 'A day of reckoning for IAB and Adtech'. *Open Rights Group*. Available at https://www.openrightsgroup.org/blog/a-day-of-reckoning-for-iab-and-adtech/

65 Digital Competition Expert Panel. (2019). *Unlocking digital competition*. UK Government. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf

66 Schweitzer, H., Haucap, J., Kerber, W. and Welker, R. (2018). *Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen*. Baden-Baden: Nomos. Available at https://www.bmwk.de/Redaktion/DE/Publikationen/Wirtschaft/modernisierung-der-missbrauchsaufsicht-fuer-marktmaechtige-unternehmen.pdf?__blob=publicationFile&v=15. An executive summary in English is available at: https://ssrn.com/abstract=3250742

67 Crémer, J., de Montjoye, Y-A. and Schweitzer, H. (2019) *Competition policy for the digital era*. European Commission. Available at: http://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf

68 Australian Competition and Consumer Commission (ACCC). (2019). *Digital Platforms Inquiry– Final Report*. Available at: https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf

69 Kerber, W. (2019). 'Updating Competition Policy for the Digital Economy? An Analysis of Recent Reports in Germany, UK, EU, and Australia'. *Social Science Research Network*. Available at: https://ssrn.com/abstract=3469624

70 Digital Competition Expert Panel. (2019). *Unlocking digital competition*. UK Government. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf

71 Digital Regulation Cooperation Forum. *Plan of work for 2021 to 2022*. Ofcom. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0017/215531/drcf-workplan.pdfdata/assets/pdf_file/0017/215531/drcf-workplan.pdf

72 European Data Protection Supervisor. (2014). *Privacy and Competitiveness in the Age of Big Data. The Interplay between data Protection, Competition Law and Consumer Protection in the Digital Economy, Preliminary Opinion*. Available at: https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf

73 See: European Data Protection Supervisor 2016 initiative to create a network of data protection, consumer and competition regulators. Available at: https://www.digitalclearinghouse.org/

74 Brown, I. (2021). 'From 'walled gardens' to open meadows'. *Ada Lovelace Institute*. Available at: https://www.adalovelaceinstitute.org/blog/walled-gardens-open-meadows/

75 See: Brown, I. (2021) and Norwegian Consumer Council. (2018). *Deceived by Design*. Available at: https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/

76 Warren, E. (2020). *Break Up Big Tech*. Available at: https://2020.elizabethwarren.com/toolkit/break-up-big-tech

77 Muldoon, J. (2020). 'Don't Break Up Facebook — Make It a Public Utility'. *Jacobin*. Available at: https://www.jacobinmag.com/2020/12/facebook-big-tech-antitrust-social-network-data

78 Brown, I. (2020). 'Interoperability as a tool for competition'. *CyberBRICS*. Available at: https://cyberbrics.info/wp-content/uploads/2020/08/Interoperability-as-a-tool-for-competition-regulation.pdf and Brown, I. (2021). 'From 'walled gardens' to open meadows'. *Ada Lovelace Institute*. Available at https://www.adalovelaceinstitute.org/blog/walled-gardens-open-meadows/

79 Brown, I. (2021).

80 For a more comprehensive list, see: Brown, I. (2020). 'Interoperability as a tool for competition'. *CyberBRICS*. Available at: https://cyberbrics.info/wp-content/uploads/2020/08/Interoperability-as-a-tool-for-competition-regulation.pdf

81 European Parliament and Council of the European Union. (2022). *Digital Markets Act*, Recital 64, Article 6 (7), Recital 57, and Article 6 (9) and Recital 59. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A265%3ATOC

82 European Parliament and European Council. (2021). *Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act)*. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN

83 European Parliament and European Council. *Regulation 2019/1150 on promoting fairness and transparency for business users of online intermediation services*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R1150

84 Gatekeepers designated under the Digital Markets Act need to provide interoperability to their operating system, hardware or software features that are available or used by the gatekeeper in the provision of its own complementary or supporting services or hardware. See: European Parliament and Council of the European Union. (2022). *Digital Markets Act*, Recital 57. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A265%3ATOC

85 The Data Transfer Project is a collaboration launched in 2017 between large companies such as Google, Facebook, Microsoft, Twitter, Apple to build a common framework with open-source code for data portability and interoperability between platforms. More information is available at: https://datatransferproject.dev/

86 Digital Competition Expert Panel. (2019). *Unlocking digital competition*. UK Government. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf

87 Kerber, W. and Schweitzer, H. (2017). 'Interoperability in the Digital Economy'. JIPITEC, 8(1). Available at: https://www.jipitec.eu/issues/jipitec-8-1-2017/4531

88 Kerber, W. and Schweitzer, H. (2017).

89 Gal, M.S. and Rubinfeld, D. L. (2019), 'Data Standardization'. *NYU Law Review*, 94(4). Available at: https://www.nyulawreview.org/issues/volume-94-number-4/data-standardization/

90 Matrix.org is a recent design of an open protocol for instant messaging service interoperability.

91 Kuikkaniemi, K., Poikola, A. and Honko, H. (2015). MyData – A Nordic Model for Human-Centered Personal Data Management and Processing'. *Ministry of Transport and Communications*. Available at: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78439/MyData-nordic-model.pdf

92 Singh, M. (2021) 'India's Account Aggregator Aims to Bring Financial Services to Millions'. *TechCrunch*. Available at: https://social.techcrunch.com/2021/09/02/india-launches-account-aggregator-system-to-extend-financial-services-to-millions/

93 Yuchen, Z., Haddadi, H., Skillman, S., Enshaeifar, S., and Barnaghi, P. (2020) 'Privacy-Preserving Activity and Health Monitoring on Databox'. *EdgeSys '20: Proceedings of the Third ACM International Workshop on Edge Systems, Analytics and Networking*, pp. 49–54. Available at: https://doi.org/10.1145/3378679.3394529

94 Crémer, J., de Montjoye, Y-A., and Schweitzer, H. (2019). *Competition Policy for the Digital Era. European Commission*. Available at: https://data.europa.eu/doi/10.2763/407537

95 Open Data Institute. (2016). *The Open Banking Standard*. Available at: http://theodi.org/wp-content/uploads/2020/03/298569302-The-Open-Banking-Standard-1.pdf

96 Farrell, J., and Weiser, P. (2003). 'Modularity, Vertical Integration, and Open Access Policies: Towards a Convergence of Antitrust and Regulation in the Internet Age'. *Harvard Journal of Law and Technology*, 17(1). Available at: https://doi.org/10.2139/ssrn.452220

97 Caffarra, C. (2021). 'What Are We Regulating For?'. *VOX EU*. Available at: https://cepr.org/voxeu/blogs-and-reviews/what-are-we-regulating

98 Caffarra, C. (2021).

99 Turner, S., Quintero, J. G., Turner, S., Lis, J., and Tanczer, L. M. (2020). 'The Exercisability of the Right to Data Portability in the Emerging Internet of Things (IoT) Environment'. *New Media & Society*. Available at https://doi.org/10.1177/1461444820934033

100 Efforts to standardise the 'Do Not Track' header ended in 2019 and expressing tracking preferences at browser level is not currently a widely adopted practice. More information is available here: https://www.w3.org/TR/tracking-dnt/

101 See here: https://github.com/w3c/dnt/commit/5d85d6c3d116b5eb29fddc69352a77d87dfd2310

102 European Commission. (2021). *Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act)*. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN

103 For example, search query and clickstream data.

104 Similar to 'must carry' obligations in media law, requiring, for example, a cable or satellite TV distributor to carry public service broadcasting channels.

105 Requiring, for example, a cable or satellite TV distributor to show competitors' channels equally prominently in Electronic Programme Guides as their own.

106 Davies, S. and Trend, L. (2020). *The Poverty Premium: A Customer Perspective*. University of Bristol Personal Finance Research Centre. Available at https://fairbydesign.com/wp-content/uploads/2020/11/The-poverty-premium-A-Customer-Perspective-Report.pdf

107 Ezrachi, A. and Reyna, A. (2019). 'The role of competition policy in protecting consumers' well-being in the digital era'. BEUC. Available at: https://www.beuc.eu/publications/beuc-x-2019-054_competition_policy_in_digital_markets.pdf

108 While there is an emerging field around 'structured transparency' that seeks to use privacy-preserving techniques to provide access to personal data without a privacy trade-off, these methods have not yet been proven in practice. For a discussion around structured transparency, see: Trask, A., Bluemke, E., Garfinkel, B., Cuervas-Mons, C. G. and Dafoe, A. (2020). 'Beyond Privacy Trade-offs with Structured Transparency'. *arXiv*, Available at https://arxiv.org/pdf/2012.08347.pdf

109 In 2017, Uber launched the Uber Movement initiative, which releases free-of-charge aggregate datasets to help cities better understand traffic patterns and address transportation and infrastructure problems. See: https://movement.uber.com/

110 See: LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique (1). Available at: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033202746/

111 Nahles, A. (2019). 'Digital progress through a data-for-all law'. *Social Democratic Party*. Available at: https://www.spd.de/aktuelles/daten-fuer-alle-gesetz/

112 See: Chapter 7 of Part 5 of the Digital Economy Act and UK Statistics Authority. 'Digital Economy Act: Research and Statistics Powers'. Available at: https://uksa.statisticsauthority.gov.uk/digitaleconomyact-research-statistics/

113 European Parliament. (2022). *Digital Services Act*, Article 31. Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0269_EN.html

114 European Commission. (2021). *Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act)*. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN

115 European Commission. (2021). Articles 4 and 5.

116 European Commission. (2021). *Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act)*, Article 5(2). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN

117 European Parliament and Council of the European Union. (2022). *Digital Markets Act*, Article 6 (9) and (10). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A265%3ATOC

118 Benesch, S. (2021). 'Nobody Can See Into Facebook'. *The Atlantic*. Available at: https://www.theatlantic.com/ideas/archive/2021/10/facebook-oversight-data-independent-research/620557/

119 Benesch, S. (2021).

120 See: Harvard University. *Social Science One*. Available at: https://socialscience.one/

121 Silverman, C. (2019). 'Exclusive: Funders Have Given Facebook A Deadline To Share Data With Researchers Or They're Pulling Out'. *BuzzFeed*. Available at: https://www.buzzfeednews.com/article/craigsilverman/funders-are-ready-to-pull-out-of-facebooks-academic-data

122 Timberg, C. (2021). 'Facebook made big mistake in data it provided to researchers, undermining academic work'. *Washington Post*. Available at: https://www.washingtonpost.com/technology/2021/09/10/facebook-error-data-social-scientists/

123 Ada Lovelace Institute. (2021). *Algorithmic accountability for the public sector*. Available at: https://www.adalovelaceinstitute.org/report/algorithmic-accountability-public-sector/

124 Ada Lovelace Institute. (2022). *Algorithmic impact assessment: a case study in healthcare*. Available at: https://www.adalovelaceinstitute.org/report/algorithmic-impact-assessment-case-study-healthcare/

125 A famous example is ProPublica's bias audit of a criminal risk assessment algorithm. See: Angwin, J., Larson, J., Mattu, S. and Kirchner, L. (2016). 'Machine Bias – There's software used across the country to predict future criminals. And it's biased against blacks'. *ProPublica*. Available at https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

126 A recent audit of Twitter looked at how its algorithm amplifies certain political opinions. See: Huszár, F., Ktena, S. I., O'Brien, C., Belli, L., Schlaikjer, A., and Hardt, M. (2021). 'Algorithmic amplification of politics on Twitter'. *Proceedings of the National Academy of Sciences of the United States of America*, 119 (1). Available at: https://www.pnas.org/doi/10.1073/pnas.2025334119

127 Ada Lovelace Institute. (2021). *Technical methods for regulatory inspection of algorithmic systems in social media platforms*. Available at: https://www.adalovelaceinstitute.org/report/technical-methods-regulatory-inspection/

128 Kayser-Bril, N. (2020). 'AlgorithmWatch forced to shut down Instagram monitoring project after threats from Facebook'. *AlgorithmWatch*. Available at: https://algorithmwatch.org/en/instagram-research-shut-down-by-facebook/ and Albert, J., Michot, S., Mollen, A. and Müller, A. (2022). 'Policy Brief: Our recommendations for strengthening data access for public interest research'. *AlgorithmWatch*. Available at: https://algorithmwatch.org/en/policy-brief-platforms-data-access/

129 Benesch, S. (2021). 'Nobody Can See Into Facebook'. *The Atlantic*. Available at: https://www.theatlantic.com/ideas/archive/2021/10/facebook-oversight-data-independent-research/620557/

130 Ada Lovelace Institute and Reset. (2021). *Inspecting algorithms in social media platforms*. Available at: https://www.adalovelaceinstitute.org/wp-content/uploads/2020/11/Inspecting-algorithms-in-social-media-platforms.pdf

131 Micheli, M., Ponti, M., Craglia, M. and Suman A.B. (2020). 'Emerging models of data governance in the age of datafication'. *Big Data & Society*. doi: 10.1177/2053951720948087

132 Shah, H. (2018) 'Use our personal data for the common good'. *Nature*, 556(7699). doi: 10.1038/d41586-018-03912-z

133 Martinez, M. and Kirchner, L. (2021). 'The Secret Bias Hidden in Mortgage-Approval Algorithms'. *The Markup*. Available at https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms

134 See: Uber Movement initiative. Available at: https://movement.uber.com

135 Coyle, D. (2022). 'The Public Option'. *Royal Institute of Philosophy Supplement*, 91, pp. 39–52. doi:10.1017/S1358246121000394

136 Ada Lovelace Institute. (2021). *Exploring legal mechanisms for data stewardship*. Available at: https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/

137 Ada Lovelace Institute. (2021).

138 Ada Lovelace Institute. (2021). *Exploring legal mechanisms for data stewardship*. Available at: https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/ and Micheli, M., Ponti, M., Craglia, M. and Suman, A. B. (2020). 'Emerging models of data governance in the age of datafication'. Big Data & Society. doi: 10.1177/2053951720948087

139 Pozen, D. and Khan, L. (2019). 'A Skeptical View of Information Fiduciaries'. *Harvard Law Review*, 133, pp. 497–541. Available at: https://harvardlawreview.org/2019/12/a-skeptical-view-of-information-fiduciaries/

140 Pozen, D. and Khan, L. (2019).

141 Shkabatur, J. (2018). 'The Global Commons of Data'. *Social Science Research Network*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3263466

142 Miller, K. (2021). 'Radical Proposal: Data Cooperatives Could Give Us More Power Over Our Data'. *Human-Centered Artificial Intelligence* (HAI), *Stanford University*. Available at: https://hai.stanford.edu/news/radical-proposal-data-cooperatives-could-give-us-more-power-over-our-data

143 European Parliament and Council of the European Union. (2022). *Regulation 2022/868 on European data governance (Data Governance Act)*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868&qid=1657575745441

144 European Parliament and Council of the European Union. (2022). Recital 30. For a more detailed discussion on the mandatability of data rights, see: Giannopoulou, A., Ausloos, J., Delacroix, S. and Janssen, H. (2022). 'Mandating Data Rights Exercises'. *Social Science Research Network*. Available at: https://ssrn.com/abstract=4061726

145 Council of the European Union. (2022). *Data Governance Act explained*. Available at: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained

146 European Parliament and Council of the European Union. (2022). *Data Governance Act*, Recital 33. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868&qid=1657575745441

147 For example, Workers Info Exchange's plan to set up a 'data trust', to help workers access and gain insight from data collected from them at work. Available at: https://www.workerinfoexchange.org/. See more broadly: Ada Lovelace Institute. (2021). *Exploring legal mechanisms for data stewardship*. Available at: https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/ and Ada Lovelace Institute. (2021). *Participatory data stewardship*. Available at: https://www.adalovelaceinstitute.org/report/participatory-data-stewardship/

148 See: MyData. *Declaration of MyData Principles*, Version 1.0. Available at: https://mydata.org/declaration/

149 European Parliament and Council of the European Union. (2022). *Data Governance Act*, Recital 27. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868&qid=1657575745441

150 Sadowski, J. (2020). 'The Internet of Landlords: Digital Platforms and New Mechanisms of Rentier Capitalism'. *Antipode*, 52(2), pp.562–580.

151 Keegan, J. and Ng, A. (2021). 'There's a Multibillion-Dollar Market for Your Phone's Location Data'. *The Markup*. Available at https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data

152 Kavi, A. (2021). 'The F.T.C. votes to use its leverage to make it easier for consumers to repair their phones'. *The New York Times*. Available at: https://www.nytimes.com/2021/07/21/us/politics/phones-right-to-repair-FTC.html

153 Sadowski, J., Viljoen, S. and Whittaker, M. (2021). 'Everyone Should Decide How Their Digital Data Are Used — Not Just Tech Companies'. *Nature*, 595, pp.169–171. Available at https://www.nature.com/articles/d41586-021-01812-3

154 Sadowski, J. (2022). 'The political economy of data intermediaries'. *Ada Lovelace Institute*. Available at https://www.adalovelaceinstitute.org/blog/political-economy-data-intermediaries/

155 OECD. (2020). *Innovative Citizen Participation and New Democratic Institutions: Catching the Deliberative Wave*. doi:10.1787/339306da-en

156 Ada Lovelace Institute. (2021). *Participatory data stewardship*. Available at: https://www.adalovelaceinstitute.org/report/participatory-data-stewardship/

157 Gastil, J. (ed.). (2005). *The deliberative democracy handbook: strategies for effective civic engagement in the twenty-first century*. Hoboken, N.J: Wiley.

158 IAP2 International Federation. (2018). *Spectrum of Participation*. Available at: https://www.iap2.org/page/pillars

159 Ada Lovelace Institute. (2022). *Algorithmic impact assessment: a case study in healthcare*. Available at: https://www.adalovelaceinstitute.org/wp-content/uploads/2022/02/Algorithmic-impact-assessment-a-case-study-in-healthcare.pdf

160 Islam, S. (2021). '"Brussels So White" Needs Action, Not Magical Thinking'. *EU Observer*. Available at: https://euobserver.com/opinion/153343 and Azimy, R. (2020). 'Why Is Brussels so White?'. *Euro Babble*. Available at: https://euro-babble.eu/2020/01/22/dlaczego-bruksela-jest-taka-biala/

161 Çetin, R. B. (2021). 'The Absence of Marginalised People in AI Policymaking'. *Who Writes The Rules*. Available at: https://www.whowritestherules.online/stories/cetin

162 European Commission. (2020). *EU Anti-Racism Action Plan 2020-2025*. Available at: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-anti-racism-action-plan-2020-2025_en

163 Çetin, R. B. (2021). 'The Absence of Marginalised People in AI Policymaking'. *Who Writes The Rules*. Available at: https://www.whowritestherules.online/stories/cetin

164 Meyer, L. (2021). 'Nothing About Us, Without Us: Introducing Digital Rights for All'. *Digital Freedom Fund*. Available at: https://digitalfreedomfund.org/nothing-about-us-without-us-introducing-digital-rights-for-all/ ; Niklas, J. and Dencik, L. (2021). 'What rights matter? Examining the place of social rights in the EU's artificial intelligence policy debate'. *Internet Policy Review*, 10(3). Available at: https://policyreview.info/articles/analysis/what-rights-matter-examining-place-social-rights-eus-artificial-intelligence; and Taylor, L. and Mukiri-Smith, H. (2021). 'Human Rights, Technology and Poverty'. *Research Handbook on Human Rights and Poverty*. Available at: https://www.elgaronline.com/view/edcoll/9781788977500/9781788977500.00049.xml

165 Corporate Europe Observatory, (2021). *The Lobby Network: Big Tech's Web of Influence in the EU*. Available at: https://corporateeurope.org/en/2021/08/lobby-network-big-techs-web-influence-eu

166 For more information about citizens' assemblies see: Involve. (2018). *Citizens' Assembly*. Available at: https://www.involve.org.uk/resources/methods/citizens-assembly. For an example of how public deliberation about complex technologies can work in practice, see: Ada Lovelace Institute. (2021). *The Citizens' Biometrics Council*. Available at: https://www.adalovelaceinstitute.org/report/citizens-biometrics-council/.

167 Wood, G. (2014) 'ĐApps: What Web 3.0 Looks Like'. Available at: http://gavwood.com/dappsweb3.html

168 See: BitTorrent. Available at: https://www.bittorrent.com/

169 Aramonte, S., Huang, W. and Schrimpf, A. (2021). 'DeFi risks and the decentralisation illusion.' *Bank for International Settlements*. Available at: https://www.bis.org/publ/qtrpdf/r_qt2112b.pdf

170 Sai, A. R., Buckley, J., Fitzgerald, B., Le Gear, A. (2021). 'Taxonomy of centralization in public blockchain systems: A systematic literature review'. *Information Processing & Management*, 58(4). Available at: https://www.sciencedirect.com/science/article/pii/S0306457321000844?via%3Dihub

171 Information Commissioner's Office. (2020). 'Digital Regulation Cooperation Forum'. Available at: https://ico.org.uk/about-the-ico/what-we-do/digital-regulation-cooperation-forum/

172 And formalised through GDPR mechanisms such as codes of conduct (Article 40) and certification mechanisms (Article 42).

173 Article 25 of the GDPR.

174 Giannopoulou, A., Ausloos, J., Delacroix, S and Janssen, H. (2022). 'Mandating Data Rights Exercises'. *Social Science Research Network*. Available at https://ssrn.com/abstract=4061726

175 See: draft Indian Personal Data Protection Bill (2019). Available at: https://prsindia.org/files/bills_acts/bills_parliament/2019/Personal%20Data%20Protection%20Bill,%202019.pdf

176 See: draft Canadian Digital Charter Implementation Act (2020). Available at: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-11/first-reading

177 See: California Consumer Privacy Act of 2018. Available at: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

178 See: California Privacy Rights Act of 2020. Available at: https://iapp.org/resources/article/the-california-privacy-rights-act-of-2020

179 See: Article 38 of the South Korean Personal Information Protection Act of 2020. Available in English at: https://elaw.klri.re.kr/kor_service/lawView.do?hseq=53044&lang=ENG

180 For example, in *Lloyd v Google*, the respondent is said to have secured £15.5m backing from Therium, a UK litigation funder, to cover legal costs. See: Thompson, B. (2017). 'Google faces UK suit over alleged snooping on iPhone users'. *Financial Times*. Available at: https://www.ft.com/content/9d8c7136-d506-11e7-8c9a-d9c0a5c8d5c9. *Lloyd v Google* is a landmark case in the UK seeking collective claims on behalf of several millions of people against Google's practices of tracking Apple iPhone users and collecting data for commercial purposes without the user's knowledge or consent. The UK's Supreme Court verdict was not to allow collective claims, which means that every individual would have to seek legal action independently and prove material damage or distress, bearing the full costs of litigation. The full judgement is available here: https://www.supremecourt.uk/cases/docs/uksc-2019-0213-judgment.pdf

181 Solon, O. and Siddiqui, S. (2017). 'Forget Wall Street – Silicon Valley is the new political power in Washington'. *The Guardian*. Available at: https://www.theguardian.com/technology/2017/sep/03/silicon-valley-politics-lobbying-washington

182 Stacey, K. and Gilbert, C. (2022). 'Big Tech increases funding to US foreign policy think-tanks'. *Financial Times*. Available at https://www.ft.com/content/4e4ca1d2-2d80-4662-86d0-067a10aad50b

183 Clarke, L., Williams, O. and Swindells, K. (2021). 'How Google quietly funds Europe's leading tech policy institutes.' *The New Statesman*. Available at: https://www.newstatesman.com/science-tech/big-tech/2021/07/how-google-quietly-funds-europe-s-leading-tech-policy-institutes

184 Whittaker, M. (2021). 'The steep cost of capture'. *ACM Interactions*. Available at: https://interactions.acm.org/archive/view/november-december-2021/the-steep-cost-of-capture

185 Ada Lovelace Institute. (2020). *No green lights, no red lines - Public perspectives on COVID-19 technologies*. Available at: https://www.adalovelaceinstitute.org/wp-content/uploads/2020/07/No-green-lights-no-red-lines-final.pdf and Parker, I. (2020). 'It's complicated: what the public thinks about COVID-19 technologies'. *Ada Lovelace Institute*. Available at: https://www.adalovelaceinstitute.org/blog/no-green-lights-no-red-lines/

186 Ada Lovelace Institute. (2021). *Exploring legal mechanisms for data stewardship*. Available at: https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/ and Ada Lovelace Institute. (2021). *Participatory data stewardship*. Available at: https://www.adalovelaceinstitute.org/report/participatory-data-stewardship/

187 Data Trusts. (2020). *International approaches to data trusts: recent policy developments from India, Canada and the EU*. Available at: https://datatrusts.uk/blogs/international-policy-developments

188 See: Department for Digital, Culture, Media & Sport (DCMS). (2021). Data: *A new direction*, Section 7. Available at: https://www.gov.uk/government/consultations/data-a-new-direction

Permission to share:
This document is published under a Creative Commons licence: CC-BY-4.0

Preferred citation:
Ada Lovelace Institute. (2022). *Rethinking data and rebalancing digital power*. Available at: https://www.adalovelaceinstitute.org/report/rethinking-data/

ISBN: 978-1-7397950-5-4