WORLD ECONOMIC FORUM

Advancing Digital Agency: The Power of Data Intermediaries

INSIGHT REPORT

FEBRUARY 2022

Images: Getty Images

Contents

Disclaimer
This document is published by the World Economic Forum as a contribution to a project, insight area or interaction. The findings, interpretations and conclusions expressed herein are a result of a collaborative process facilitated and endorsed by the World Economic Forum but whose results do not necessarily represent the views of the World Economic Forum, nor the entirety of its Members, Partners or other stakeholders.

Preface

The power of the data ecosystem has never been greater but the system itself is becoming more difficult to navigate.

Anne Josephine Flanagan
Data Policy and Governance Lead, World Economic Forum

Sheila Warren
Deputy Head, Centre for the Fourth Industrial Revolution Network, World Economic Forum

Navigating the data ecosystem

The power of the data ecosystem has never been greater but the system itself is becoming more difficult to navigate due to increasing complexity. We share and receive data every day to interact with the technologies that serve us, whether in a personal or commercial context. Data value chains then funnel, use and reuse that data, usually for commercial or public interest purposes. These value chains, often involving personal data, are at best complicated to follow; at worst they can lead to mistrust in data sharing and can potentially give cover to bad actors.

Contrasted with this complexity is our reliance on data sharing both as our way of life and as the backbone of the global data economy and the key to technological innovation.

If mistrust in the data ecosystem acts as a point of failure leading to suboptimal outcomes for us all, what can be done? What if there was a better way whereby data could be more easily traced, more easily permissioned, more easily controlled by data rights holders (including people) across the data ecosystem?

Data intermediaries as a lever of action

In this report, the World Economic Forum's Task Force on Data Intermediaries, composed of business, academic and civil society actors worldwide, explores these questions and more. Building on the Forum's *Redesigning Data Privacy: Reimagining Notice & Consent for Human-technology Interaction*[1] report, the task force examines data value chain scenarios as they already exist today – and may exist in the future – with a view to improving both human–technology interaction and data sharing more broadly.

In an era that has policy-makers moving beyond just privacy laws and to grapple with developing policy levers designed to support data-sharing for common purposes, the task force shares what it has learned to support responsible policies. The value-added use of data intermediaries as a key to unlocking complexity and building trust holds the promise of protecting the interests of data sharers and data subjects alike – and ultimately that of society.

Towards trusted digital agency

Taking lessons from global business, the research community and cutting-edge technology design, we explore best practices in the use of data intermediaries. We identify various models, including the organizational data intermediary, such as the data trust, that assumes a fiduciary duty. We explore the automated gateway that predetermines standard rules. And we look to the future, to the artificially intelligent agent that allows for autonomous third-party decision-making on our behalf, with its associated promises and perils.

Finally, although any views expressed do not represent the views of any individual taskforce member or their organizations, we invite you to join us on this journey of exploration as we unearth and build a picture of where consensus may or may not lie in unleashing the power of data intermediaries leading to trusted digital agency – and where and when these types of policies could potentially be deployed.

Executive summary

Data intermediaries represent a new policy lever to navigate the challenges of the growing data ecosystem.

The challenge

Everyone is familiar with the paradigm of going online and clicking on terms and conditions they don't understand (or take time to read). No one knows (nor follows) what happens to their data. This status quo creates a reliance on companies to be responsible but can lead to mistrust in the data ecosystem as a whole. Further, mistrust between people and technology becomes amplified the more complex the data ecosystem becomes over time. Where once people had screens to navigate, new ambient data collection methods with their many benefits create nervousness and resignation when people don't have the full picture. In some cases, individuals may opt out of interacting with technologies that would be of huge benefit to their lives. But what if it were possible to outsource these decision points to a trusted agent acting on an individual's or even a group's behalf?

The opportunity

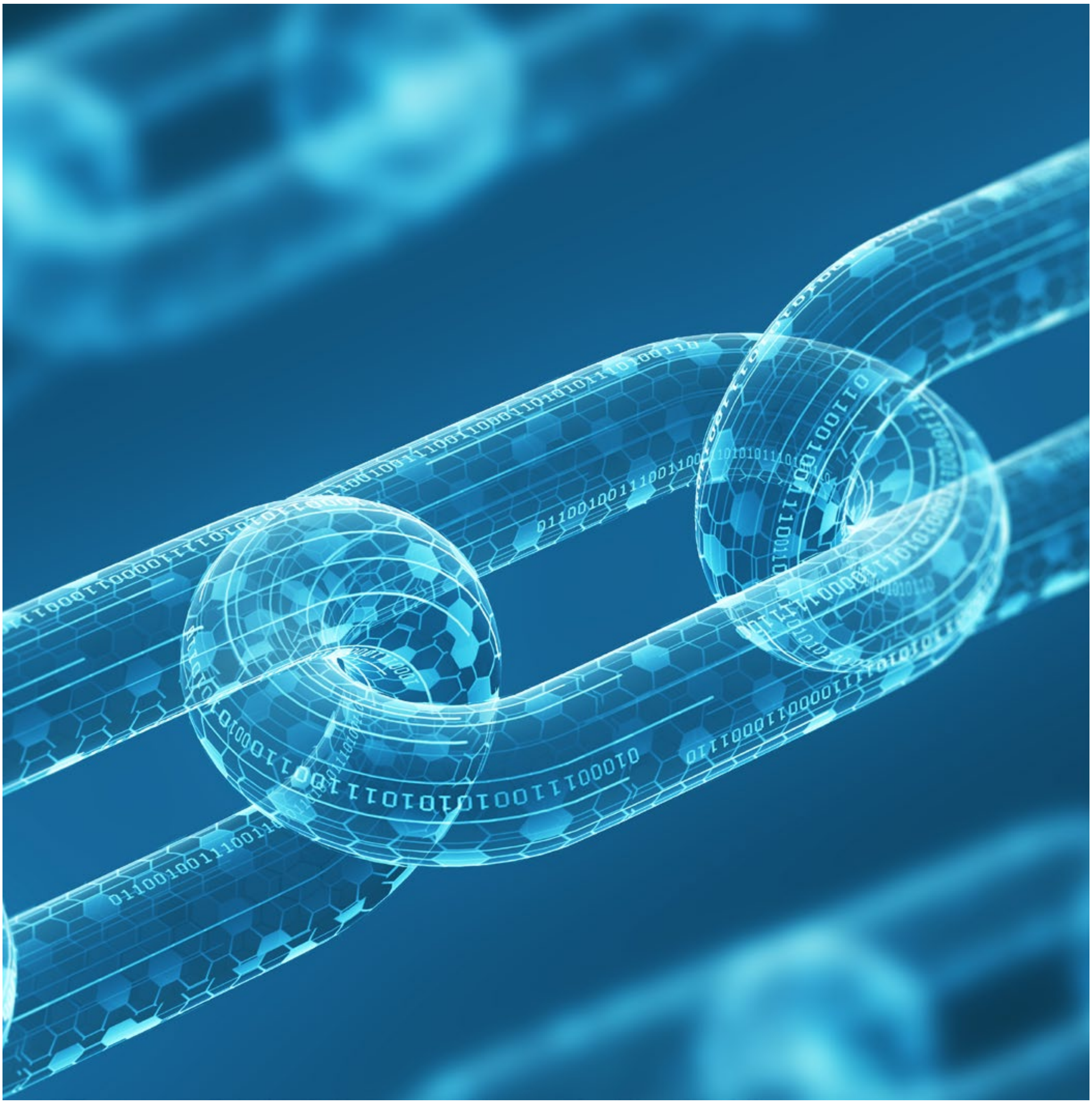
Now that screenless technology is a part of everyday life, there is an opportunity to rethink the human–technology interaction paradigm and reposition the debate to focus on roles and responsibilities beyond the person. How can the use of data intermediaries help people navigate technologies and data ecosystem models without losing sight of what it means to be human, in terms of agency and expectations? How can people think beyond that given that, as they move towards the complexity of screenless metaverse issues, their understanding of "humanness" is transforming? Data intermediaries–especially digital agents – represent a new policy lever through and around which individuals can potentially navigate the challenges of the growing data ecosystem. This report seeks to shed light on an alternative method of mediated human–technology interaction whereby data appears to travel seamlessly from people to technology in a human-centric and, crucially, trusted manner. By communicating shared incentives, establishing reputation or receiving third-party verification, as well as having assurance structures to mitigate risk to both the intermediary and the rights holders, data intermediaries can increase trust between people and the technology they interact with.

The solution

This report explores the opportunities and risks of data intermediaries and, specifically, third-party digital agents. From data trusts to trusted digital agency, the report paints a picture of a world that is more empathetic to people and to companies, providing greater certainty for data sharing as a foundation for innovation through the introduction of a trusted third party. Crucially, it suggests levers of action for both the public and private sector to ensure a future-proof digital policy environment that allows for the seamless and trusted movement of data between people and the technology that serves them.

1 The challenge: Human–technology interaction and the data value chain

Trust between parties who seek to share data is not a default state.



1.1 Introduction: The trust gap in data sharing

> People mistrust even the most responsible and ethical companies because the system – the data ecosystem – is so confusing to navigate.

"Our days are filled with myriad discrete data collection moments. Even when we have genuine intent to affirmatively consent to each moment of data collection, it is practically impossible to do so: No individual has the time to provide affirmative consent on a near constant basis. This reality arguably undermines our individual agency."[2]

The world is experiencing something of a mistrust pandemic when it comes to people's engagement with the data ecosystem. This global "trust gap" or "trust deficit" is a barrier to economic growth, digital innovation and social cohesion. The technology ecosystem is ultimately powered by the collection, sharing and processing of data, often personal in nature. Data sharing is a driver of innovation in technology and of the digitization of mature economic models.

But trust between parties who seek to share or exchange data is not a default state; it is something that needs to be earned or built, often as a result of great effort over time. This includes building trust between people and technology. It is all the more important when considering that people share data every time they interact with the technologies in their lives.

As Bill McDermott, former Chief Executive Officer of SAP, has noted: "When trust is there, we can take giant strides, turning our greatest challenges into our biggest opportunities. When it's not, the needle gets stuck. Small hurdles become insurmountable. Division overwhelms unity."[3]

As defined by Russell Hardin,[4] trust is a *belief* that an actor will perform a specific action within a specific context, whereas trustworthiness is a *property* of an actor. The goal of data intermediaries and the infrastructure that supports them is to enable data rights holders to trust *trustworthy* data intermediaries.

That is not to say that without trust and trustworthiness there is no sharing of data; but with trust and trustworthiness there will be greater participation and in turn an increase in the volume and indeed the veracity of data made available as a result.

The problem of notice & consent

“When presented with privacy notices, it is necessary to take the time to consider the implications of terms and conditions and to overcome the barrier presented by the attention required to think explicitly about preferences.

The challenges of meaningfully consenting to personal data sharing, meaning the collection and processing of personal data, are well-known.[5] Much of people’s interaction with technology relies on giving consent for data collection and processing via a medium such as a screen. When presented with privacy notices, it is necessary to take the time to consider the implications of terms and conditions and to overcome the barrier presented by the attention required to think explicitly about preferences. People need to think about what they really care about and foresee what their data might be used for – if they can imagine it. The term “decision fatigue”[6] reflects something real: Lorrie Cranor and Aleecia MacDonald of Carnegie Mellon University researched[7] the unfathomable burden of reading privacy notices that people typically experience and the resulting difficulty in being afforded the time to meaningfully react, understand and consent to them. People are simply too busy to take the time to read every consent notice on websites. And even if they did, could they truly anticipate how their data would be used?

And what if there is no screen? Ambient data collection, through for example closed circuit television and connected devices, is increasingly common. Getting to an acceptable default state is more urgent than ever as the world moves towards the creation of the metaverse where the metaphysical state of human–technology interaction becomes ever more seamless.

Other lawful bases for data collection and processing do exist in some jurisdictions, such as legitimate interest or performance of a contract under the European Union (EU) General Data Protection Regulation, but they have their own limitations. Courts the world over have been clear that notice and consent is the preferred lawful basis in certain scenarios. In situations where notice and consent has been deemed to be the only existing acceptable standard, that constraint can have limitations as described earlier.

Resultant mistrust

Today’s default state is not healthy. On the one hand, people are sometimes accepting and often left feeling disempowered; on the other hand, organizations struggle to access and process data that can meaningfully improve lives, health and even the planet.

People mistrust even the most responsible and ethical companies because the system – the data ecosystem – is so confusing to navigate.

As for the law, it struggles to keep up. Heavily weighted in favour of principles that lack the nuance of specific scenarios, regulation’s favourite tool is simply to ask: Can this entity collect your data? And individuals say “yes” without meaningfully understanding the benefits as well as the costs, and so on and so forth as they continue to “consent” without always meaningfully consenting.

A new approach

What if there was a better way? What if you could outsource the decision-making fatigue to a trustworthy third party? What if you could pre-consent to your preferences so that you did not need to continuously opt-in? What if technology allowed you to outsource your decision-making even further – to a digitally automated agent, potentially using artificial intelligence (AI), which could actively make those decisions for you? All such scenarios require the enlisting of an intermediary.

Is the world ready for such a radical and human-centred approach to managing data relationships via a third-party data intermediary? Elements of such a sophisticated and nuanced data ecosystem already exist but the appropriate policy frameworks are far from being in place to make such a scenario viable at a systemic level.

In addition to asking this question, this report also explores the secondary effects of such a scenario through the examination of relevant use cases and asks what actions public and private sector actors can take when probing such issues for the benefit of building a more robust, human-centric and sustainable data ecosystem.

Assumptions

For the purposes of this paper, several assumptions are made.

The first assumption is that whatever the data sharing relationship, data rights holders will inherently mistrust each other without appropriate safeguards, positing that a data intermediary can potentially become that missing safeguard, depending on the data-sharing scenario and the characteristics of that intermediary. The assumption in all cases is that data rights holders have an interest in their data rights: for example, people care about information about them and companies care about the value of proprietary information.

Secondly, when exploring data intermediary possibilities, the relationships may be binary or multi-party in nature. An example of this is where data collected about people in a smart city environment can be used for the purposes of urban planning; while the people whose data was collected are themselves rights holders, the sharing takes place several times throughout a data value chain.[8]

Thirdly, it is worth nothing that data is contextual, which means that non-personal data may become personal in nature depending on the context, for example, if combined with other datasets. This includes business-to-consumer (B2C) and business-to-business (B2B) relationships involving someone’s personal data, but business-to-government (B2G) scenarios are also relevant. If data intermediaries anonymize personal data and/or handle non-personal data, it may be recommended that they should have a process in place to test the robustness of their anonymization methodology. Nevertheless, given the difficulty of disassociating personal data from data sets that contain otherwise non-personal data, and the higher regulatory bar placed on the handling of personal data, personal data will be used as a proxy for all data.

And finally, there is no silver bullet approach: policy responses are as nuanced as the scenarios they respond to. It is assumed that the findings of this work as they pertain to personal data may be adjusted as relevant to apply to the treatment of different scenarios, including exclusively non-personal data-sharing scenarios, such as B2B sharing of proprietary data generated from non-personal data sources or unknown future use cases. Indeed, it is intended that this paper be made available to contribute to future work by others in this space.

1.2 Introducing data intermediaries

The possibilities of a mediated approach to data sharing by a third party are as limitless as the possibilities of data sharing itself. Data intermediaries can empower people to control and even automate the flow of data about themselves, improve cross-border data flows, and allow for the leveraging of personal data for social impact, to name just a few use cases.

Data intermediaries can take many forms; but what they share is a primary purpose of facilitating and managing data relations between data rights holders (such as people or businesses), depending on the parties' relationships, intentions and resources. They do so by encapsulating, communicating and enacting the shared interests of the relevant parties and safeguarding their interests. At their most basic level they facilitate the exchange of information; at their most sophisticated they can assume decision-making, including on behalf of people.

By definition, it is assumed that data intermediaries are always third party in nature, as witnesses to the primary data sharing transaction.

How specific data rights holders may benefit from data intermediaries

To facilitate trust between data rights holders, at the most basic level data intermediaries may communicate shared incentives, establish reputation or receive third-party verification; and have assurance structures in place to mitigate risk to both the intermediary and the rights holders.

In addition, they can take on different roles for different kinds of data rights holders.

BOX 1 **The role of data intermediaries for different data rights holders**

People & society
A data intermediary can play a significant role in enabling people to be more in control of their personal data, determining what personal data is shared with which participants and for what purposes. They can vet parties that would receive the data to determine if they are "trusted" based on a set of externally published standards and criteria, thereby removing the obligation from the individual and thus removing the deficiency of the notice and consent mechanism common in data protection regimes. A data intermediary can leverage economies of scale to implement technologies to enable greater protection of personal data through real-time anonymization, pseudonymization[9] or other privacy enhancing technologies and services. Conversely, the data intermediary could also verify and confirm the identity of the individual, thereby providing additional guarantees that the information being shared belongs to the individual and has not been misappropriated or obtained by other means.

Data intermediaries could also provide a variety of services, including that of matchmaker between supply and demand for data. They could engage in security, authentication and fraud prevention activities, such as performing verification services on the participants and the data being introduced based on a range of parameters, from potential copyright infringement to information security scanning of malicious code.

Businesses & private sector organizations
A data intermediary can act as a conduit to gain greater access to permissioned personal data. It can also enable greater sharing of that data between private corporations and organizations. Private entities could benefit from the use of a data intermediary as a method of third-party verification that complies with a set of base standards, such as those as determined by a sector or industry: this is already the case in relation to information security and the tracking of illegal activity online. A data intermediary can also help participants navigate laws, regulations and other complex data privacy requirements, thereby effectively outsourcing some of these services to the intermediary. It is for this reason that there has been a boom in so-called "regtech" whereby third-party processes manage information compliance. Such third parties could be classified as private data intermediaries.

In a similar vein, scientific research institutions have been proponents of data trust models for a number of years, given that the data trust can act as a trustworthy conduit to manage access to data that otherwise would be inaccessible for purposes other than research.[10] This paper examines data trusts in more detail later.

Government & public sector bodies
Although there is growing momentum to enable greater sharing of public data by government bodies, this remains sporadic and, where personal data is involved, complex and limited. Open data policies seek to streamline access to publicly held data but often fall short. The World Economic Forum's recent work on empowered data societies,[11] sheds light on this topic through the example of improving access to publicly held data in the City of Helsinki. One finding of that work is that citizen-held data can be a rich source of relevant information for government service provision and can enhance people's lives by delivering value for societies if conducted in a human-centric manner. A data intermediary can help ensure trust in such a scenario.

Advanced competencies of data intermediaries

The above are just a few main examples of the usefulness of data intermediaries. Some of the more advanced competencies of data intermediaries may include:

- Storing individuals' personal data within a personal data space or a vault so that data processing can happen within that space without the transmission of personal data to any parties outside the space; rather the insights from the data are transmitted in a manner similar to federated data learning models. Echoes of this idea appear in a proposal for Common European Data Spaces.[12]

- Advising individuals on uses of their data, including tracking who is uses their data and for what purpose.

- Strengthening individuals' negotiation power when influencing the terms of the data use(s), negotiating a "fee" for the data exchange, or solving disputes.

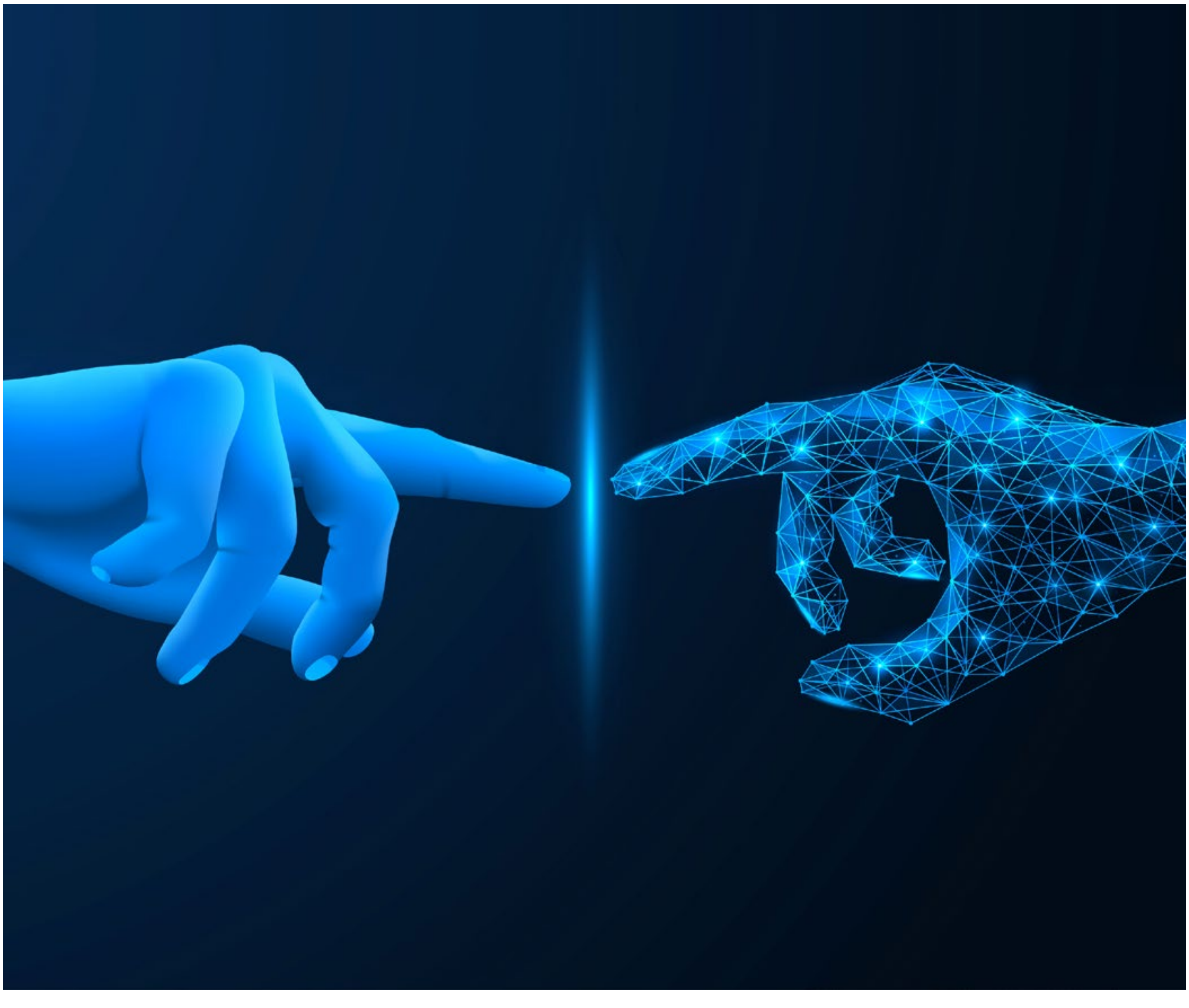
- Leverage individuals' personal data for social impact, such as to contribute to academic or scientific research.

- Providing added-value services to participating members, such as data anonymization and/or aggregation, benchmarking services, security and fraud prevention.

- Acting as a data aggregation and/or pseudonymization and/or anonymization layer.

- Acting as a proxy for consent to offer individual control to the data subject.

If data intermediaries can add so much value, why are they not used more often? One possible answer is the complexity of the data value chain within which date intermediaries operate by definition and the policy environment surrounding both it and the data ecosystem as a whole.



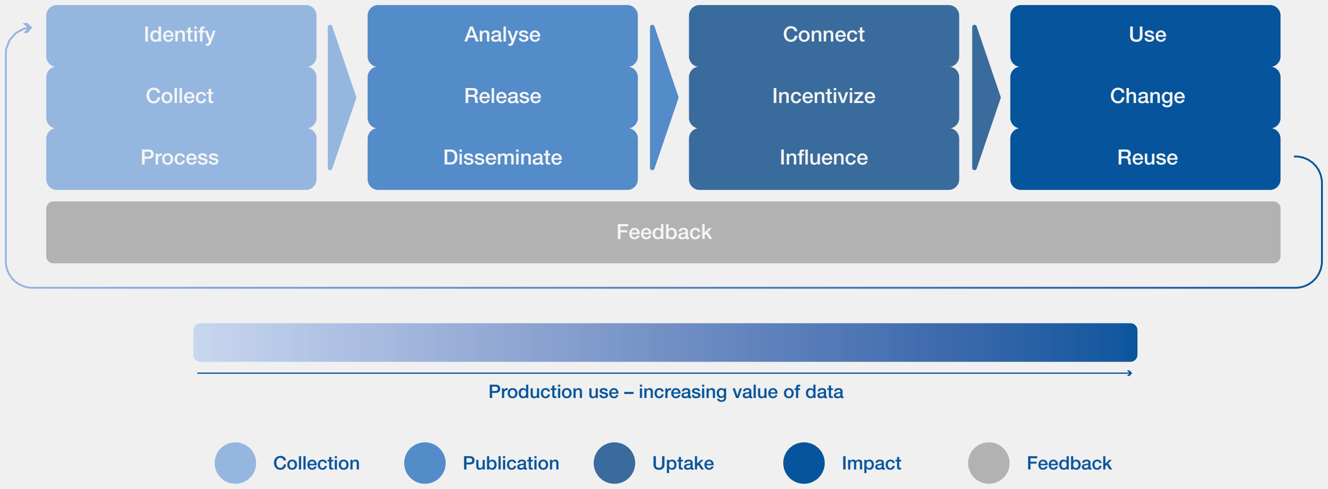
1.3 Exploring data value chains

The data ecosystem versus the data value chain

In describing the difference between the data ecosystem and a data value chain, the former might be termed as all data, all transactions and the global space within which data exists and is processed, whereas the latter is a value chain of sorts. Data exists in the data ecosystem by default, but once data is collected and processed it enters a data value chain and that value chain is as long and as infinite as the life of the data.

Open Data Watch's data value chain model below describes the four major stages of the life cycle of data: collection, publication, uptake and impact. In addition, as data is an infinite resource and (absent external constraints) can be reused infinite times in infinite ways, the model also contains a feedback loop. This feedback loop is something everyone is familiar with: it is the means by which functional data sharing takes place and how technology knows what to serve back. It has implications for online advertising, profiling and, taken to the extreme, is key to dark patterns (which combine heretofore disparate data sets for purposes of manipulating the user in a non-transparent manner). But importantly, without this feedback loop it would be impossible for people to interact with today's technologies in any meaningful fashion. In other words, the feedback loop is a neutral feature of the data value chain but may be open to manipulation. Disposing of data closes the feedback loop.[13]

FIGURE 1 Open Data Watch's Data Value Chain[14]



Beyond notice & consent: How a data intermediary alters the flow of data in a data value chain

> “ **Once automated decision-making starts to occur, a type of synthetic data precedent arises. This means that a data-use pattern emerges that infers further use cases.**

Introducing a data intermediary into the data value chain can fundamentally alter the flow of data in the transaction by disrupting at least one point in the chain.

Under the notice and consent model, a person consents to the collection and processing of their data at the very beginning of the data value chain. The data then flows through the data value chain, guided by the permissions set before the data entered the chain.

A data intermediary could alter this process in several fundamental ways. If the purpose of a data intermediary is to effectively accompany personal data by adding a layer of permissioning onto the accompanying metadata (or use metadata as a proxy), that permissioning effectively follows the data (technically it acts to determine the use of the data) throughout the entirety of the data value chain and will trigger changes on a case-by-case basis depending on what the permissioning allows for. A similar model is in use in permissioned and permissionless blockchains.

Below are some different variations of permissioning scenarios in the data value chain using data intermediaries:

1. **Notice & consent:** This is the default state whereby people consent to the collection and processing of personal data. There are alternative lawful bases for data collection and processing but in all cases a pre-determination is made that the data can lawfully enter the data value chain.

2. **Transferred permissioning:** The data intermediary could take the data into a brand-new data value chain by relying on the permissions from previous unrelated incidents of data collection and processing by the same person. This alters the collection phase of the data value chain (identify, collect, process) by leapfrogging past specific notice and consent.

3. **Pre-permissioning using digital identity:** This mimics transferred permissioning above, except now the power of digital identity is introduced. For example, if someone’s digital identity stored their general preferences for data collection and processing, then any time that digital identity interacted with relevant scenarios those preferences and permissioning could be taken forward by a data intermediary to conduct brand new transactions. The value of this is that the person does not need to be asked more than once what their preferences are; but an obvious downside is that the use cases may be very different from each other and consent is being inferred, which may reduce individual agency and lead to unintended outcomes.

4. **Automated decision-making by a digital agent:** In this scenario a data intermediary digital agent takes on the role of decision-maker. Consent is automated as before but this time using AI the data intermediary agent decides autonomously what kind of data permissioning a person might like. This opens the door to even more possible uses of that data. This type of scenario disrupts the normal flow of data in the data value chain at all stages and again can carry both wonderful opportunities and considerable risks. The key to success here lies in the quality of the automated decision-making and the underlying algorithm.

5. **Replenishing and automating across multiple data value chains:** Once automated decision-making starts to occur, a type of synthetic data precedent arises. This means that a pattern of data use emerges that infers further use cases. If this could be harnessed at a systemic level with appropriate policy safeguards, the data and its associated permissions could be recycled over and over and look slightly different every time but should reflect the preferences of the user. The move is towards a fully automated system of personal data collection and processing to overcome notice and consent limitations. This is a scary and amazing space and arguably not so different from a world absent of any data protection and privacy requirements: the difference here is that there is a system, ideally with backstops, designed in a human-centric manner and therefore retains the preferences of the user and exerts limits accordingly. In fact, there is no reason AI agents could not be programmed to be conservative if that is what is reflective of the user’s preferences. In addition, such a system would require clear rules to avoid a conflict of interest on the part of the digital agent.

Important note on best practice

When it comes to personal data, most data protection and privacy regimes do not currently allow for many of the above scenarios. In most jurisdictions that use the notice and consent model, consent needs to be specific and meaningful in order for the data to be considered to have been lawfully obtained. Best practice for now is therefore to avoid inferring consent where it is not explicitly and meaningfully given, regardless of the jurisdiction. Notwithstanding that other lawful grounds for the processing of personal data already exist beyond notice and consent, this paper looks at what the appropriate data intermediary backstops would need to be in order to make the above a reality. Inherent in this is the use of both public and private policy levers.

2 The opportunity: Trustworthy human-centric data intermediaries

Some common features emerge that start to build out conditions for the third-party intermediary being independent, having a set of duties in their performance, being a dedicated asset and with clear rules of the game.

2.1 Data intermediary organizational models

For human-computer interaction, researchers have developed a definition of online trust as an evolution of its offline counterpart. In the real world, “trust is the social capital that can create cooperation and coordination.”[15] In the cyberworld, trust becomes “an attitude of confident expectation in an online situation of risk that one’s vulnerabilities will not be exploited.”[16] This is at the core of the confusion of current human–technology interaction, where data collection is so ubiquitous as to make people feel at risk of being vulnerable. To solve this, intermediary third parties can be helpful.

Much can be learned from data intermediary models that are already in use in commercial and academic spheres today, whether they share personal data or not. The section below examines some of the most relevant and trusted data intermediary models already in existence at the B2B level.

– **Data stewards**

Organizational leaders such as the chief data officer may hold a designated data steward role, or teams may be empowered to ensure that data is leveraged in a responsible way. The data steward’s role is to manage data rights and data reuse, identifying opportunities for productive cross-sector collaboration and responding proactively to external requests for functional access to data, insights or expertise. Stewards are active in both the public and private sector, promoting trust within and outside their organization on how data is being used. In some cases, the data steward can be an entity with duties to carry out the interests of a group of data rights holders, a community,[17] or the entity holding the data.

To establish and demonstrate their trustworthiness, data stewards may take on a professional role, including verifiable ethics obligations or certification.[18,19] Outside organizations must always perceive the data steward as trustworthy. In the case of B2G data sharing, the data steward could even facilitate relationships between the private and public sector. Thus, the data steward can both lead responsible data management within their organization and increase the trustworthy perception of their sector and facilitate new relationships.

“ The data steward can both lead responsible data management within their organization and increase the trustworthy perception of their sector and facilitate new relationships.

– **Digital fiduciary**

A digital fiduciary takes on the mantle of duties of care and loyalty but in a somewhat different manner to a data steward and other related fiduciaries. Much as a doctor is charged with taking care of patient health or a lawyer with legal affairs, the digital fiduciary is responsible for assisting individual clients in managing their digital selves. At a minimum, this means that a digital fiduciary upholds its duty of care by doing no harm to its clients and upholds its duty of loyalty by not having any conflicts of interest. Under a more expansive definition, a digital fiduciary upholds its duty of care by protecting and enhancing the individual’s digital experiences and upholds its duty of loyalty by actively promoting the individual’s interest.[20] The digital fiduciary can be an individual or an entity, a private or public (governmental) body and, if private, a for-profit or not-for-profit enterprise.

Fiduciary duties can be defined, implemented and enforced in a variety of ways, including via: a new legal framework, existing contract law, voluntary certification, or a professional association with licensing and related assurance infrastructure (like for physicians or lawyers).

– **Data trust**

A data trust is a repeatable framework of agreements based on trust or contract law, allowing data rights holders to delegate control of their data to a trustee.

If the data trust employs trust law, the trustee is bound by fiduciary duties of loyalty and care to act in the interest of the beneficiary. The trust pools individuals’ power and provides an agent to negotiate their interests, suited to managing individuals’ asymmetric relationships with companies in a complex technical environment. Upholding duties of loyalty requires the data trust to be independent and may preclude the data trust from being a for-profit company. Although trust law does not exist in all countries, fiduciary duties are more common globally.[21] A data trust can be designed for different levels of beneficiary participation, delegating various degrees of decision-making power to the trustee.[22] A data trust contract then is “a contract among one or more controllers of data (the ‘entrusters’) and a third party under which the entrusters empower the third party (the ‘data trustee’) to make certain decisions about use or onward supply of data (the ‘entrusted data’) on their behalf, in the furtherance of stated purposes that may benefit the entrusters or a wider group of stakeholders (such entrusters or stakeholders being referred to as the ‘beneficiaries’).”[23]

- **Data collaborative**

  A data collaborative is a data sharing relationship that can take multiple forms, including public interfaces, a trusted intermediary, data pooling, research and analysis partnerships, prizes and challenges, and intelligence generation. In a relationship between organizations of different sectors, the data collaborative allows for one or more parties' data, insights, models or expertise to be shared.[24] A data collaborative encourages data sharing by enabling public interest use of previously siloed data. While the sharing could be multidirectional between multiple varying parties, data collaboratives most often refer to private sector entities sharing data with the public sector or with public interest groups. Incentives for corporations to share data include reciprocity in data access, research insights, reputation, revenue through data collaborative agreements, regulatory compliance or philanthropy and corporate social responsibility (CSR), or environmental social and governance (ESG).

- **Data cooperative**

  A data cooperative is a network of agreements between peers with mutual interests, allowing data resources to be pooled.[25] Members bring in data and are responsible for stewarding the data. Data is brought and removed as members join and leave.[26]

- **Data commons**

  A data commons is a network of relationships between data rights holders who have equal rights to a common, indivisible data resource. The structure follows Elinor Ostrom's eight principles for governing commons,[27] as follows:

  1. Boundaries of users and resource are clear
  2. Congruence between benefits and costs
  3. Users had procedures for making own rules
  4. Regular monitoring of users and resource conditions
  5. Graduated sanctions
  6. Conflict resolution mechanisms
  7. Minimal recognition of rights by government
  8. Nested enterprises

The data is an undivided resource and members have equal rights to the data; thus, the data remains unchanged despite members joining and leaving.[28]

Public versus private models

“ Can a data intermediary be truly independent, especially in relation to the services it may offer and the financial incentive to perform?

Some common features emerge that start to build out conditions for the third-party intermediary being independent, having a set of duties in their performance, being a dedicated asset and with clear rules of the game. Considering the difference also in various duties of care from model to model, does it make a difference whether the intermediary is public or private in nature? Can a data intermediary be truly independent, especially in relation to the services it may offer and the financial incentive to perform? The following section explores some further characteristic options, especially as they relate to human–technology interaction and the collection and processing of personal data.

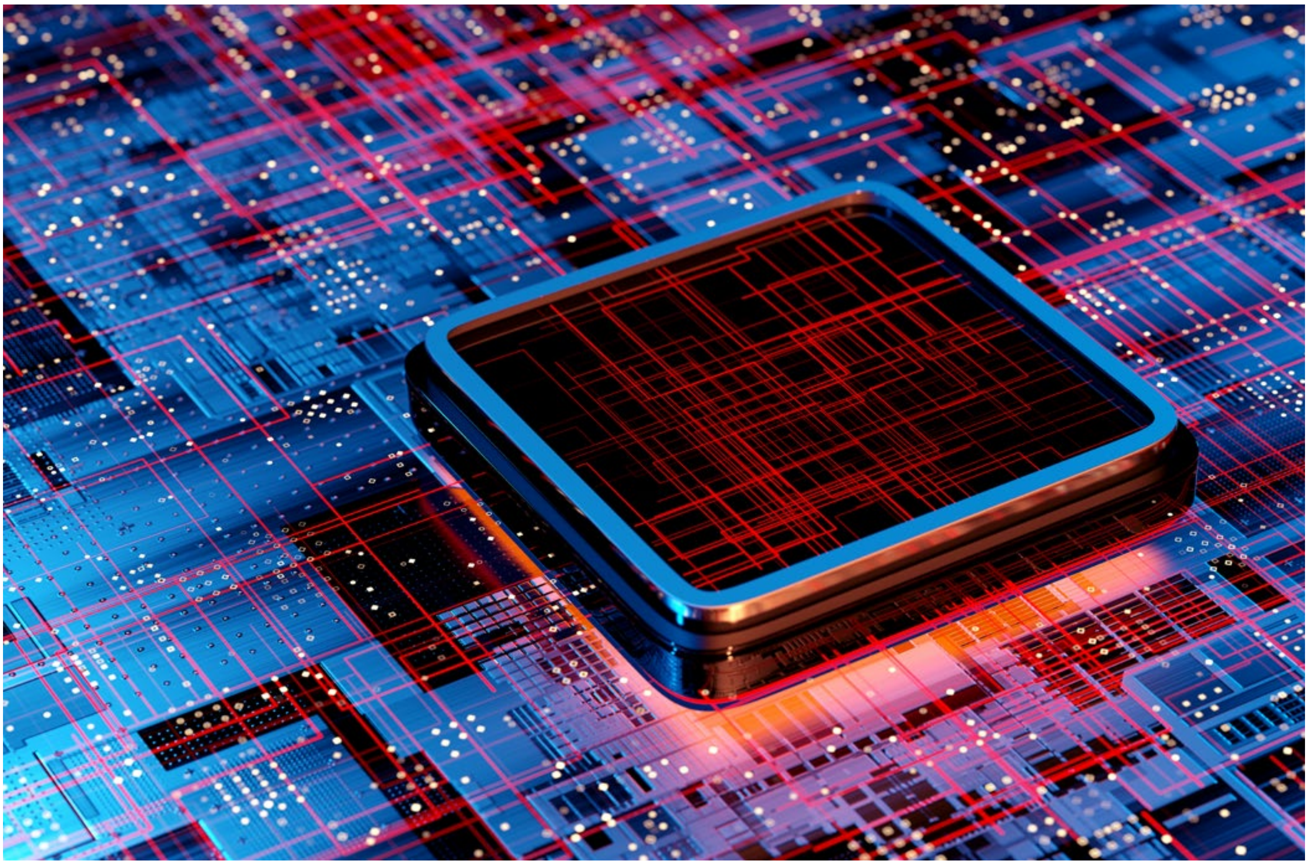
– Public data intermediaries

A public body or government agency could take on the role of an intermediary, especially as it relates to data coming from public bodies. Therefore, it can also act as an aggregator or gateway for such information. Such an intermediary could play an even greater role in making the data more easily accessible, identifiable, searchable and usable, including coordinating interoperable systems, especially across the public sector at least. Therefore, the role of a public body is arguably greater if it is an aggregator of multiple sources of public data. Another role it could play is to act as a super-intermediary, setting the national standard, data architecture and data standards for which all organizations would be required to comply. This will require deep expertise in privacy, data and technology, and therefore upskilling of the staff and/or hiring of a “data steward” with the required skillsets.

However, whether a public body can be said to be “trusted” will be dependent on the role of government in any given country, its level of control, access and use of surveillance laws and related technologies. Although a super-intermediary may enable vast sharing of data between multiple participants, enabling economies of scale and a consistent interoperable approach even across borders, if there is no trust in the system, in the government and its underlying intentions, there may not be active use, unless under the force of law. This would then impact the veracity of data being shared and could in turn stifle innovation.

– Private for-profit data intermediaries

Whether and how a for-profit commercial entity can successfully serve its clientele under voluntary fiduciary duties of care and loyalty remain open to debate among stakeholders.[29] A key driver of the success of this model is how the intermediary derives economic value to be able to perform and make this service available.



Without strict controls on the access, use and transfer of the underlying data provided by data ecosystem participants, this model could incentivize the intermediary to examine ways to profit from the data itself, unless prohibited by law or contractual arrangements. Where a participation fee may not generate sufficient profit, the provision of additional services could satisfy the economic argument without requiring any service that involves or enables the intermediary to profit from the data itself, directly or indirectly. A hybrid of this approach and variation of cost models could bridge this issue. Various models could also co-exist, with a certification or trust mark for those that abide by certain agreed standards. On the other hand, however, is an immense opportunity for the most responsible organizations that could be incentivized to create or pay a trusted third-party intermediary to increase their independence and transparency with respect to their user base and thus commercial appeal with respect to offering services to their users.

- **Non-profit data intermediaries**

  A non-profit data intermediary will need to be economically viable to exist and cover ongoing costs. An independent non-profit intermediary may be preferable as a third-party neutral body, with the usual caveats of a successful non-profit.

2.2 The policy environment

Governments are starting to pay attention to the idea of trusted intermediary bodies to support data sharing. The new European Union Data Governance Act "aims to foster the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU."[30] The Government of the United Kingdom also recently commissioned a report[31] on data intermediaries that has determined they can empower both people and businesses in data sharing activity. As governments seek to regulate data sharing, agile, innovative and positive solutions will be needed.

" Governments are starting to pay attention to the idea of trusted intermediary bodies to support data sharing.

A key question in more broadly actualizing data intermediaries that can eventually act as digital agents for people will be the role of assurance structures in facilitating trustworthiness. Legal frameworks, whether statutory or contractual, can act as assurances to limit harm to data rights holders and provide a safer ecosystem for building trust but are insufficient on their own. Thus, other forms of assurance, such as professional codes of conduct, licensing and adherence to social norms, may be necessary to establish trustworthiness among intermediaries.

In the area of human–technology interaction, a majority of governments worldwide have already established baseline data protection and privacy requirements, even if there are differences between jurisdictions. Some governments are now also regulating automated decision-making via AI legislation. There is also much to be learned from parallel policy areas beyond data protection and privacy:

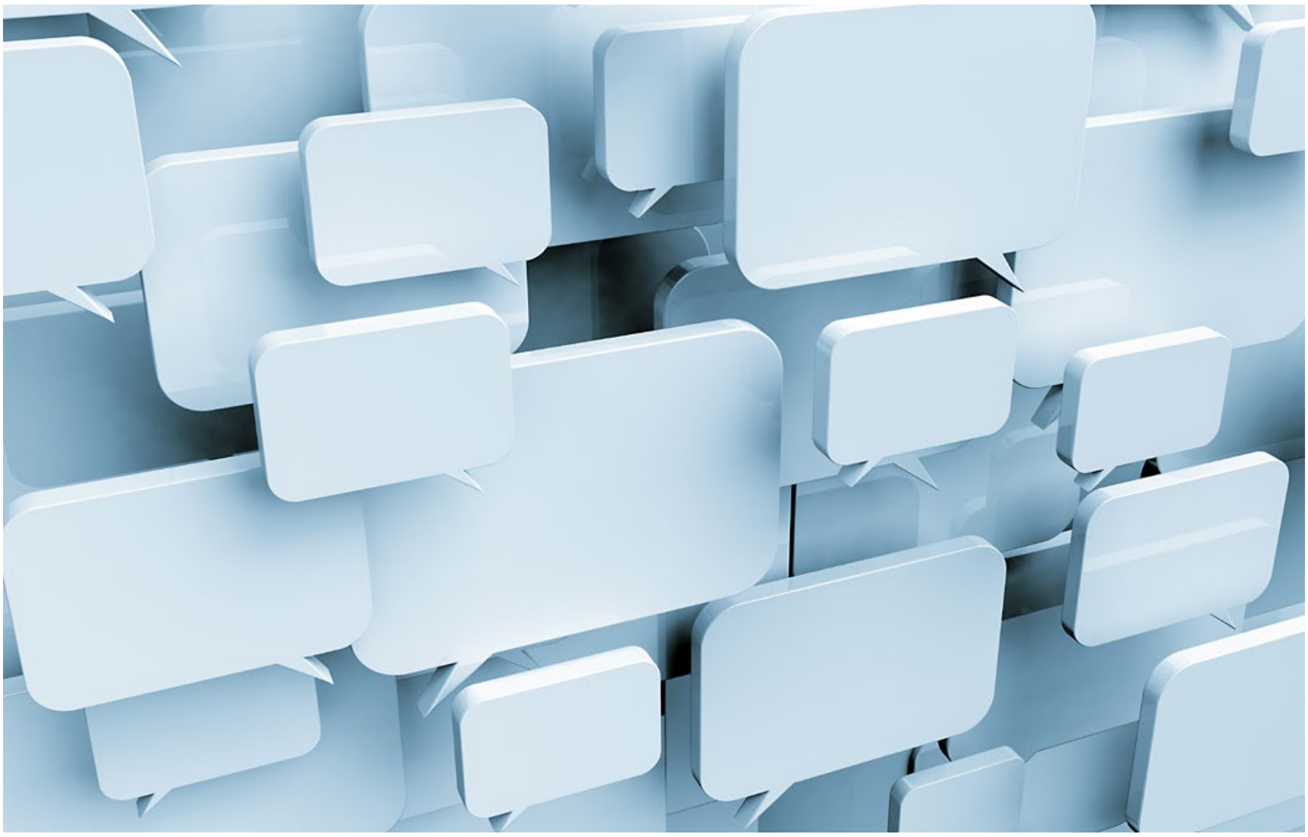
- **Human rights law –** Data intermediaries in Europe must comply with human rights law (e.g. European Union Charter of Fundamental Rights), for example by ensuring data intermediary services do not result in unfair bias and discrimination

- **Antitrust and competition law** – The data intermediary could not be used as a vehicle to share or disclose materially sensitive information between competitors. On the other hand, data intermediaries could serve as effective antitrust remedies to address market failures and incumbent platform companies.

- **Intellectual property law** – The data intermediary could protect the trade secrets and intellectual property rights of data sharing participants

- **Data localization requirements** – The data intermediary may need to process/store certain types of data "on soil", meaning within a country/region (e.g. Russia, China)

Driven by the recognition of the importance of the data economy, it is clear that many governments understand the significance of making data available for innovation; at the same time, policy ambitions to promote data sharing are coming to light. However, because that often involves the sharing of personal data, data protection and privacy issues continue to be important. But data protection and privacy are highly evolved areas of policy-making, so it will be interesting to see how policy in the area of trusted data intermediaries evolves to take account of this tension.



2.3 Human-centricity and fiduciary duty

What might creating safeguards for data intermediaries look like in reality? Two complementary concepts come to the fore: human-centricity and fiduciary duty.

Human-centricity

"Human-centricity means focussing on something variously called (self-)sovereignty, self-determination, self-governance, autonomy, agency or the like, in terms of the people involved with the generation of data. These concepts derive from the internationally-recognized concepts of human rights. A human-centric approach is one that makes central the following: that people have the right to determine, without any kind of coercion or compulsion, what happens to them."[32]

Autonomy and agency are core tenets of human-centricity and fit in with the aims of restoring trust to human–technology interaction. Human-centric design is a well-researched and used space but human-centricity has typically taken a backseat to a rights-based approach when it comes to data protection and privacy norms, especially when it comes to regulation.

Fiduciary duty

A more highly developed area of consideration is fiduciary duty. A fiduciary typically abides by two basic types of duties: care and loyalty.
In turn, these can be further subdivided into four specific duties:

- The general tort-like duty of care = do no harm to others
- The fiduciary duty of care = act prudently towards the entrustor
- The "thin" fiduciary duty of loyalty = have no conflicts of interest between duties and clients
- The "thick" fiduciary duty of loyalty = promote the entrustor's best interests.

Importantly, because fiduciary duties are considered relational, they run not with property but with the person and their entrusted confidence.

While those are primary duties, others also have been recognized.[33] These include confidentiality (keeping confidences shared during the course of the fiduciary relationship) and good faith (a catch-all for having the right intentions).[34] Unlike a contract, a fiduciary duty could foreseeably be perpetual in nature, as in the case of lawyers and doctors whose fiduciary duty continues even after the contract ends.

The law of fiduciaries does not exhaust the common law as a rich source of rights and responsibilities. Other potential common law-based sources of intermediary duties/rights include torts, bailment and misappropriation. Indeed, a policy framework that matches the duties to the specific digital concern being addressed can be envisioned.

One approach is to conceive of the responsible and trustworthy data intermediaries desired in the data ecosystem – or at least the person at the data intermediary responsible for trustworthy data processing – as having the role of "data stewards".

BOX 2

Liability: A tricky question

By managing collectively massive amounts of data originating from many data sources, data trusts are not in a position to assess the legality of all the uses of the data that are made. They are consequently exposed to liability risks in a way that can be compared to the liability of other online platforms for the illegal content that they contribute to sharing.

The risk of liability of data trusts could further be managed by designing appropriate dispute resolution mechanisms that shall apply in case of legal disputes affecting data trusts. It is essential to ensure that the complex disputes that may arise in connection with the use of data in the context of data trusts (e.g. misappropriation of data, loss of data, access to data vs protection of confidentiality) and that may involve multiple parties (data holders, data trusts and data users) shall be solved in a cost-efficient and coordinated manner. This could be done by creating dedicated global alternative dispute resolution mechanisms (including arbitral tribunals) that would be better equipped – compared to national courts or national regulatory bodies[35] – to solve "data disputes" (i.e., disputes about the use of data).[36] Multi-territorial alternative dispute resolution systems would make it possible to avoid the geographic fragmentation that would result from (parallel) national court litigation/ national regulatory proceedings. Alternative dispute resolution mechanisms consequently offer a most convenient and attractive tool to address the challenges of what has been called "massive online micro-justice"[37] (i.e. the challenges resulting from the need to manage a multitude of small (micro) disputes, as is done in the digital online environment with respect to content moderation on digital platforms).[38] Proposals have been made to set up specific dispute settlement mechanisms, including dispute review boards.[39]

3 Moving towards trusted digital agency

Digital agents may negotiate access to data above and beyond a simple binary gated function.

3.1 The role of digital identity in supporting human agency

Can the use of data intermediaries establish a notion of sort of "digital self-determination[40]" by helping people navigate technologies and data ecosystem models without losing sight of what it means to be human, in terms of agency and expectations? Our digital identities may hold the key to allowing us to determine how we can start to navigate the data ecosystem around us in a more sophisticated manner.

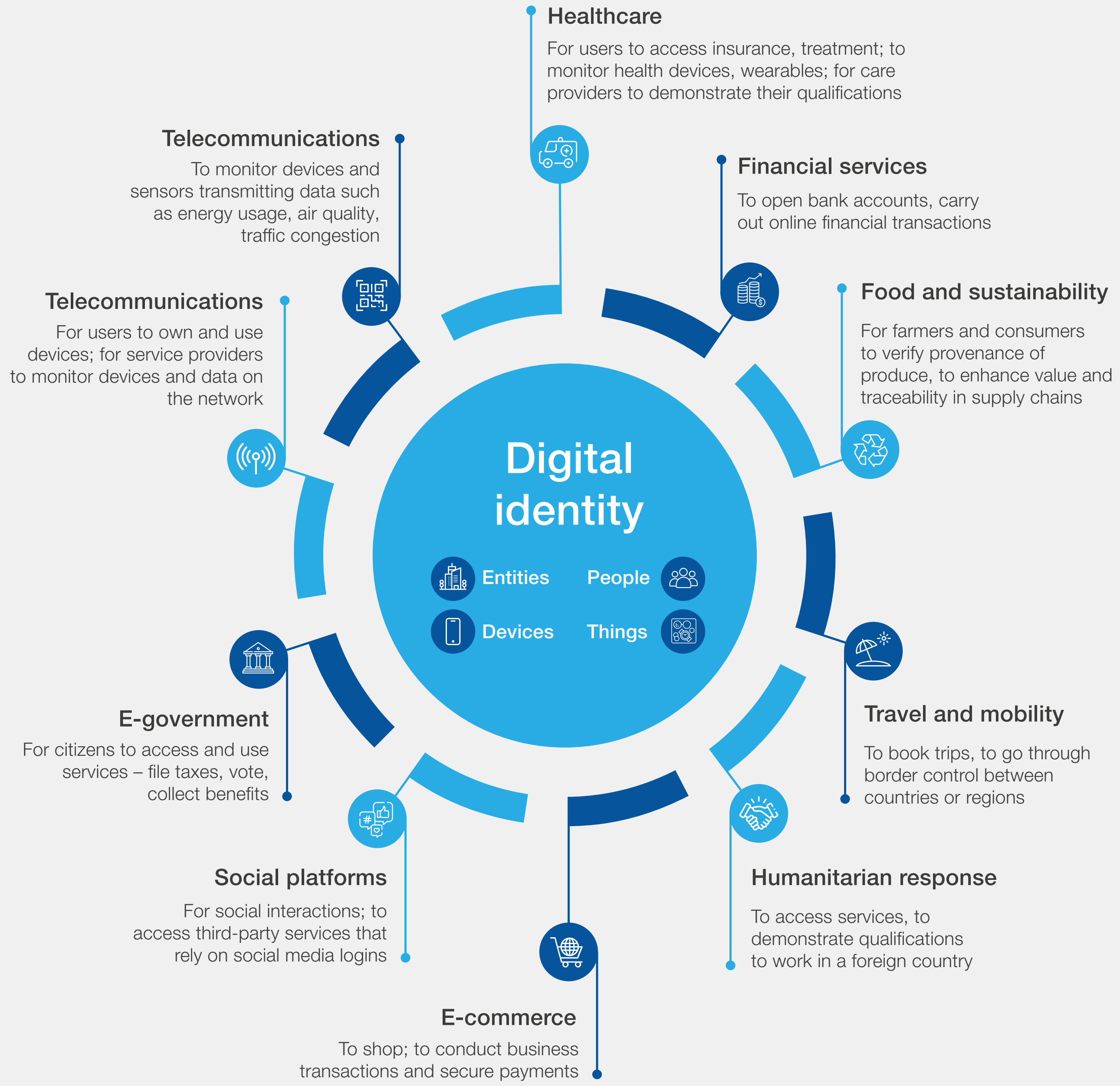
Digital identity

A digital ID is the electronic equivalent of an individual's identity card. It is a way to provide verified personally identifying information of an individual for a software to read and process. Both online and offline environments can adopt digital identity. And it can also act as a key by storing and deploying permission.

Carefully designed and properly managed, digital ID can also enhance privacy protection and reduce the rise of identity fraud since each time only minimum information is needed for authentication for the specific purpose. Some of the biometric based digital ID systems have already been adopted in financial transactions and for a cash-free shopping experience. Such authentication and authorization processes can be completed in real time and free of hassle.

Good digital identity has five key components as defined by a multistakeholder group curated by the World Economic Forum: useful, inclusive, secure, offers choice, fit for purpose.[41] Figure 2 shows the importance of Identity in everyday lives.

FIGURE 2 Identity in everyday lives


Healthcare
For users to access insurance, treatment; to monitor health devices, wearables; for care providers to demonstrate their qualifications
Telecommunications
To monitor devices and sensors transmitting data such as energy usage, air quality, traffic congestion
Financial services
To open bank accounts, carry out online financial transactions
Telecommunications
For users to own and use devices; for service providers to monitor devices and data on the network
Food and sustainability
For farmers and consumers to verify provenance of produce, to enhance value and traceability in supply chains
Digital identity
Entities
People
Devices
Things
E-government
For citizens to access and use services – file taxes, vote, collect benefits
Travel and mobility
To book trips, to go through border control between countries or regions
Social platforms
For social interactions; to access third-party services that rely on social media logins
Humanitarian response
To access services, to demonstrate qualifications to work in a foreign country
E-commerce
To shop; to conduct business transactions and secure payments

Source: *World Economic Forum, 2018,* Identity in a Digital World A new chapter in the social contract.

BOX 3 Digital identity has an evolving scope[42]

Authentication: Processes that determine if authenticators used (e.g. fingerprints, passwords) to claim an identity are valid. Sometimes digital identity goes beyond authentication. Authentication is a security process that compares attributes to confirm a claim. In principle, there is no need to know who the person is. In digital identity, there may be a need to link the person to their identity and that may require identity verification technologies.

Profile: May include inherent data attributes (such as biometrics) or assigned attributes (such as names or national identifier numbers).

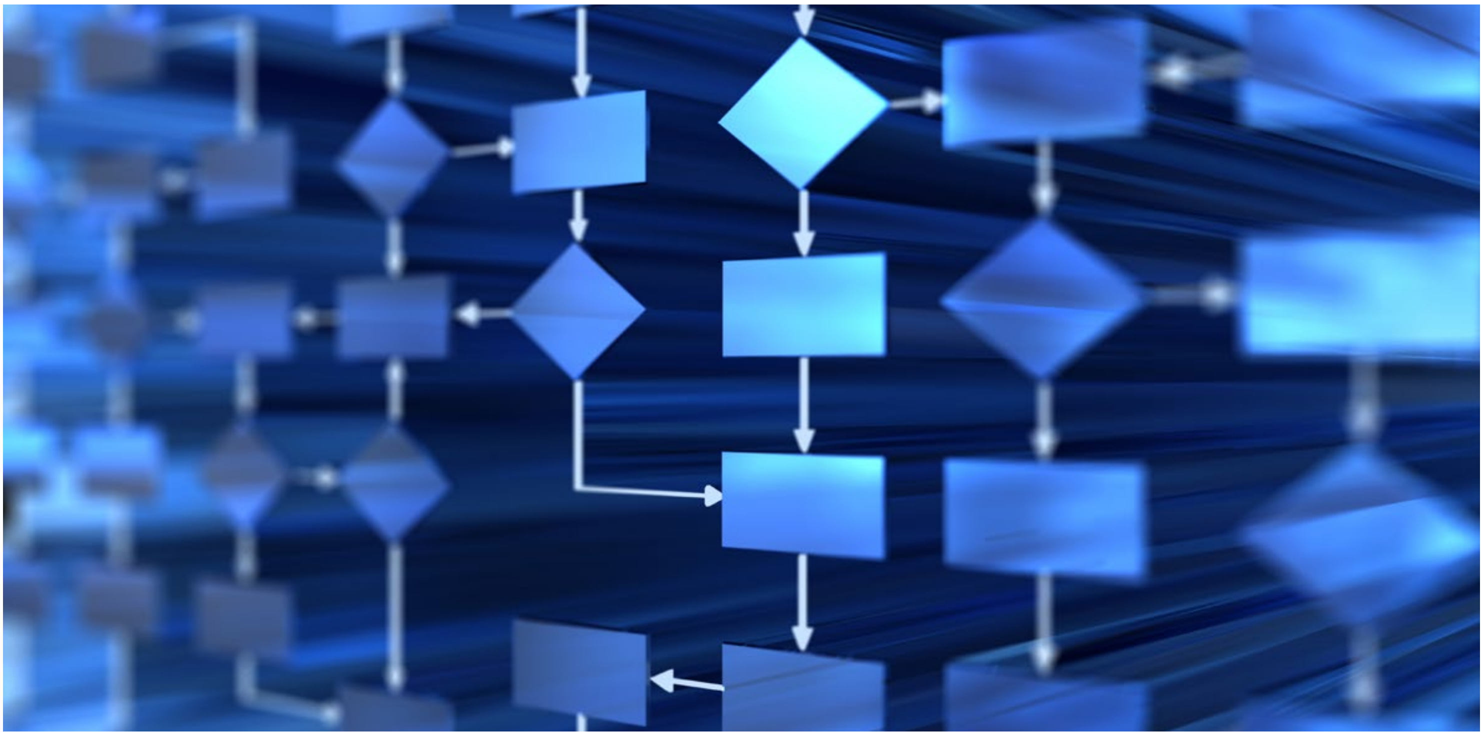
History: Credit or medical histories, online purchasing behaviours.

Inferences: Judgements or decisions made based on authentication processes, profiles and histories (e.g. a bank decides the attractiveness of an individual for a loan).

Individuals can already use decentralized identity solutions, for example, personal data servers to import their personal data and on-device data storage, from banking and healthcare information to social media data, and use them directly for identity authentication and data access authorization with apps and websites.[43] This technology can empower users to take control of their personal information, increasing data portability.

TABLE 1 **Evolutions in digital identity solutions and how they can help**

	Now	Evolution	Future
Digital ID	**Consent** Traditional intermediaries and user consent (e.g. web browsers, apps, mobile devices)	**Shift control to user** Personal data stores, on-device data storage and more advanced data intermediaries (e.g. smart devices, agents)	**Agency** Next level of data intermediaries (embedded in body, devices, homes, cities, etc.)
Characteristics	– Focus on Verified Attributes (address, age, health status) – Governance: centralized, distributed, federated – Looser data stores (e.g. profile built by larger tech companies, by browsers) – Self-declared attributes (e.g. social media login)	– More collaborative digital ID approaches (within sectors, e.g. health, banking; at national levels, e.g. across borders; or at regional levels, e.g. travel corridors, trust): – Personal data stores (e.g. Digi.Me) focusing on consumer to business (C2B) and user control, reducing need for business-to-business (B2B) interactions – User-driven web (e.g. Solid project) and embedding digital ID into the web experience – Query-based ID (e.g. Demos UK), avoiding data exchange, just answer queries “are you over 18?”, “are you vaccinated”, etc.?	– A fundamental level of ID proofing and verified attributes remains (I am really who I say I am) – Focus shifts from only verified attributes and credentials to profiles and inferences about a person – Fluid boundaries between data stores, agents and data managed on individual’s behalf – Evolving definition of control/agency – Needs scalable user agency concepts
Policy considerations	– Data protection and privacy – Security requirements – Data minimization – Certification of issuers, verifiers	– Credential interoperability (technical, legal levels) – Legal acceptance of digital ID – Trust frameworks linked to attributes, exchange of credentials – Recourse and liability	Create definitions and thresholds of ownership, delegation, liability Prescribe transparency, auditability, predictability Allow for scalable (rule-based vs granular per data items) approaches to scope of data agency Create sandboxes for experimentation



How digital identity helps solve decision fatigue and improve data sharing potential in human–technology interaction

Digital identity can allow for the selection of preferences and the making of certain choices in advance, such as "pre-consent", avoiding doubling of efforts. This already happens in device usage: when setting up a new phone, for example, users can predetermine privacy settings before using any app. Their identity is usually inherently connected to their devices. Similarly, through the use of cookies, browsers can remember which user is which through a set of identifiers.

Digital identity then can be the key to unlocking a less ethically concerning but arguably equally impactful scenario as an AI-enabled digital agent. Digital identity allows the digital agent to recognize that the data belongs to a specific user and consult the permissions that that user has authorized (effectively data processing scenarios that the user has pre-consented to) and act accordingly in line with the user's wishes. Crucially, consent can be given in advance for a myriad of use cases and that consent can be attached to the user's digital ID.

BOX 4

Vaccine passports

The COVID 19 pandemic has led to a heightened focus on the power of medical data, specifically so-called vaccine passports. These passports by nature serve as a form of digital identity. Commercial entities serve as a type of centralized data intermediary in several jurisdictions. Given the sensitivity of this type of health data, in many cases governments have procured third-party contractors to administer and manage such systems. Unsurprisingly, strict security and privacy criteria are central to such systems in most cases, not least because a public policy health concern relies on increasing trust in the system.

Such vaccine passports are used when travelling between jurisdictions and at a local level, such as when entering dining establishments or other places where proof of vaccination status is necessary. Importantly, these intermediaries provide a means of verifying status without sharing health data with the establishment per se, in a sort of zero-knowledge proof scenario whereby the trusted data intermediary verifies that the data subject is vaccinated but does not share any other information. This avoids unwanted secondary effects of the establishment sharing the data any further.

However, at a collective level, vaccine data is an incredible public health asset. The United Kingdom Government in particular has acknowledged this[44] and has suggested that anonymization, pseudonymization and data shielding techniques could be harnessed in a controlled environment to allow for the reuse of that highly sensitive data. In such cases, notice and consent is not required per se for the reuse of the data but the intermediary processes the data undergoes must be done in a controlled environment so that the findings of the data set are made available rather than the data itself.

3.2 Automated decision-making

Machine decisions vs human decisions

To automate the data intermediary process there are some additional concerns about machine decision-making that people may inherently distrust due to the machine's lack of empathy.[45] In addition, as well as perceived harm, as the Future of Privacy Forum points out, harms associated with automatic algorithmic decision-making can vary.[46]

So how to instil trust? It comes down to backstops of governance including provisions for recourse and mechanisms for redress. The rules of a banking transaction – the execution of standardized and consistent behaviour throughout the transaction– acts as a de facto data intermediary because the data is handled through a specific process with rigorous backstops. This example plays out especially in the payments industry, where people rely on trusted third-party technology to handle money and the data that represents the value of that money. Nowhere is this truer than in blockchain technology and cryptocurrency, where the value of assets is intangible and inherently and inextricably fully dependent on trusted data.

Many different technologies could potentially serve a role as an intermediary; but some of the most interesting and relevant are those acting as software agents. A software agent is defined by four key hallmarks: autonomy, social ability, responsiveness and proactiveness.[47]

Excitingly, digital agents may negotiate access to data above and beyond a simple binary gated function. Using sophisticated algorithms may allow for decisions that emulate agency and autonomy in as close a way to human decision-making as possible.

BOX 5

The four key hallmarks of a software agent[48]

Autonomy: Agents should be able to perform the majority of their problem-solving tasks without the direct intervention of humans or other agents; and they should have a degree of control over their own actions and their own internal state.

Social ability: Agents should be able to interact, when they deem appropriate, with other software agents and humans in order to complete their own problem solving and to help others with their activities where appropriate.

Responsiveness: Agents should perceive their environment (which may be the physical world, a user, a collection of agents, the internet, etc.) and respond in a timely fashion to changes that occur in it.

Proactiveness: Agents should not simply act in response to their environment; they should be able to exhibit opportunistic, goal-directed behaviour and take the initiative where appropriate.

3.3 A potential trusted digital agency model

In order to be truly at the service of the individual, a trusted digital agent (TDA) that automates permissions for people and effectively manages their data across different services needs to respect a certain number of rules. Below is an outline of a prototype concept of how such a TDA might work.

CASE STUDY

Meet Valexander, a TDA

Rules of the game for Valexander, a friendly, trustworthy TDA

The TDA will base its decisions mostly upon:

- Previous consents and preferences of the person, as well as the full context of such consents (who, what, when, why, etc.).
- Previous consents and preferences of the large amount of people that agent serves.
- Information about the person (age, gender, objectives, etc.).
- Information about the services it exchanges data to and from:
  - Nature of the service
  - Type of organization
  - Business model
  - What data is needed by the service when and why.

Such a TDA needs to guarantee:

- Neutrality on the services it recommends
  - The business model of the TDA should not depend on the services it shares data to and from in order to guarantee its neutrality.
- Compliance for data sharing
  - Data sharing needs to be compliant with regulation, sectoral rules, contracts and governance frameworks.
  - While the TDA may perform basic compliance checks, it is unlikely to be able to conduct full-fledged compliance reviews. For instance, for personal data to be shared lawfully under the General Data Protection Regulation (GDPR), the data must have been collected lawfully in the first place (by the data provider) and the data may not be used for incompatible purposes (by the data user). This is a complex area and must be nuanced, so the TDA is best seen as supplementary to compliance itself.
  - The TDA should therefore be able to perform a basic check that compliance exists before any data sharing occurs, with the caveat that a verifiable third party likely conducted the compliance itself.
  - Such checks could be traced using smart contracts on the chain, for instance.
  - TDAs should have contracts with people guaranteeing it serves their best interests.
- Auditability, explainability of its processes
  - The TDA needs to be able to explain why it shared data with one service and not with another.
  - It needs to be able to list the criteria it based its decisions on.
  - While this is not always entirely possible with machine learning/deep learning (ML/DL) technologies, inputs need to be clear and explainable and there needs to be accountability of the TDA.
- Human interaction for some data sharing
  - On some sensitive or crucial data sharing (regarding the type of data or type of processing that will occur), the person needs to validate the data sharing.
- Accuracy of the data shared
  - Since, for instance, the TDA will allow people to easily keep their profiles up to date, it needs to make sure data shared is always accurate and up to date or provide some grade on the accuracy of the data.
  - This will be possible when the data provider is the data holder/subject but less so when the data provider is an organization.
- Interoperability with other TDAs
  - People need to be able to easily change TDAs without losing their preferences, just as it is possible to change telecom providers without losing the number.

To enable this, governance is needed. This governance is larger than the TDA or the organization that develops it. It includes the person and the public and private organizations that form a legitimate and representative alliance to make such decisions (public-private-people partnership).

Possible suggestions to ensure good governance of TDAs:

- TDAs could be registered at the appropriate authority and precise requirements should be installed, as well as audits and certifications.
- TDAs could be interoperable and rely on open standards. Non-compliance should be fined and prosecuted. Liabilities should be clear for the organization developing the TDA.
- TDAs should be neutral and independent in regard to the digital services that will use the person's data, in order to prevent any conflict of interest and ensure the TDAs only serve the interests of the person.
- The person can manage and decide its preferences on the data, reset any profile the TDA is supposed to use, and needs to be able to reverse an automatic decision made by the TDA or made in consequence of the TDA's decision.
- Governance structures (public-private-people partnerships) need to be mandated or created to decide and standardize:
    - When human interaction is necessary
    - The automatic decisions that can be reversed and how
    - Governance rules, standard contracts and agreements for TDAs
    - How consents and preferences are stored
    - Interoperability standards of the TDAs
    - Certifications for TDAs
    - Business models of TDAs guaranteeing neutrality of TDAs for the digital services
    - The public information about the digital services the TDA will share data to and from:
    - What data is needed, when it is needed, why does each service need it and what is the business model?
    - How is that information described and provided? For instance, for the health sector there should be a registry so that health services (public and private) register that information.
    - This will guarantee fair access to data about the services needed by TDAs, explainability of the TDA's decision and foster competition among TDAs.
- It is essential to ensure a person can change their TDA and that there is competition among TDAs:
    - People can easily switch from one TDA to another without losing their preferences or profile. TDAs can differentiate on the quality of their AI but not on the data they access about the person or about the services.

In the case of a sophisticated approach like the one above, TDA interoperability must be mandatory in order for this system to function. But Valexander is just one example: this paper's role is to unearth the opportunities and risks of TDAs as the world moves towards trusted digital agency that is not just interesting from a technical and policy perspective but may become essential in one form or another.

4 Reshaping human-technology interaction

The use of a data intermediary to overcome the limitations of notice and consent does not do away with the core components of notice and consent but merely displaces them.

4.1 How the use of data intermediaries shapes human–technology interaction

“ The system should be accessible, interrogable, intelligible and controllable.

Designing for online interfaces and interactions relies upon existing heuristics. Such heuristics have remained largely unchallenged despite developments in both the underpinning business models of online platforms and data protection law. Even when designing to support user consent, the rule of minimal distraction (that a designer should seek to ensure the user is not distracted or noticeably redirected from their principal activity/goal) remains a tenet.[49] However, when the locus of consent is distributed or redirected, as in the case of data intermediaries, this then requires substantial rethinking of how to approach the design of such interactions. At its most basic, a priori consent requires that the user be cognizant of the transaction, informed of its implications, and capable of agreeing to the terms.

One might assume that if a data intermediary is sought, then this is a voluntary choice (and ultimately revocable); therefore, the moral role of interaction designers is not to replicate consent but simply to scaffold understanding and promote agency,[50] so as to ensure that any signal of assent is sufficiently supported. This notion of informational sufficiency is highly contextual but broadly includes: (a) how much a user should understand and the presentation of this information; (b) what aspects of the system or the data transfers should be highlighted/brought to the surface and how/when this might occur; and (c) when and how to alert users to changes in system state. Another way to consider this is to first ask: “How much do I need to know to ensure I am neither surprised nor upset by the use of my data?” The second question to ask is: “How soon, and in what way, would I wish to know this?”

Another way to look at this issue is through human data interaction (HDI), a normative framework intended to reduce the overarching issues into three principles: agency, legibility and negotiability.[51] HDI pushes individuals beyond user awareness and control, extending this to include questions over how a user might interrogate the system in order to support their understanding and then how the user might allow the system to exert control over how their data is used. Arguably, even if a data intermediary distributes consent, the user should still be unsurprised by what happens, be able to interrogate the model, and have the tools available that allow them to act, if they so choose. So, the system should be accessible, interrogable, intelligible and controllable.

Finally, the use of a data intermediary, to overcome the limitations of notice and consent, does not do away with the core components of notice and consent but merely displaces them. Informing, agency and revocation (awareness and control) are still central to the functioning of an effective intermediary. Equally, agreeing to trust such a system with data requires a priori assent but with the additional burden of informational sufficiency, as with any software product. However, given the normative nature of such a system, it is also necessary to consider how to design the onboarding/assent process to be one more akin to an engagement with any offline intermediary. While such relationships are notoriously difficult to model through systems design, one interesting concept is that of building in latency, or the affordance of delay, in the law and the design of computational systems.[52]And the “ongoing pursuit of seamless user experiences forecloses opportunities for engagement with the text, meaningful reflection, suspicion and interrogation, thereby limiting agency and autonomy,”[53] raising the importance of building moments of latency into interaction design, particularly in the build-up to assent.

4.2 User experience design consequences of using a third-party digital agent

The design for which a digital agent framework becomes universally accessible and desirable must follow a traditional approach to achieving ease of use. To a greater degree when dealing with digital identity and personal data, there exists a challenge of trust and participation, which makes it vital to achieve a low rate of attrition.

Beginning with the user, there must be a high degree of individual control and open knowledge developed into the framework to ease concerns of surveillance, misuse and security vulnerabilities.

To the first point of surveillance, a data intermediary could be designed as a pass-through mechanism without knowledge of the data exchanged, where no access to the data is required for the service. Producers of data will be sceptical of each point of interaction between producer and consumer, thus creating a need for open design.

With a blurred reality of liability and consequences for data misuse, a decentralized exchange system such as blockchain must be incorporated to enhance security and limit siloed control. The responsibility of intermediaries to act on behalf of both parties creates a need to establish well-checked decentralized transaction and decision-making processes throughout the entire exchange. Whether government, enterprise, private company or individual, trust must be earned and security proven through the design of a framework that includes the following attributes:

Useful: A portable and responsive design that functions across platforms and is acceptable to less tech-savvy users.

Inclusive: A universal, non-discriminatory and accessible tool that allows ease of use and inhibits exclusion, and whose design prevents surveillance.

Secure: A trusted and open framework that is auditable and designed with a dashboard that provides notifications of all data access points.

Choice: A user-centric and user-managed design where alternatives are provided through informed consent.

Purpose: The accuracy and sustainability of design that encourage use across services over time, with predictable outcomes.

The EU's Data Governance Act proposes a framework for the governance of data intermediaries, including the obligation to have neutral and independent data intermediaries, interoperability of data intermediaries, registration and specific governance organizations.

Initiatives are emerging to unite data intermediaries and public and private service providers to form such governance organizations and start building those rules for automatic human-centric data sharing. For example, in the European Union, aNewGovernance unites leaders of such TDAs and organizations in the skills (education, employment, etc.) and mobility sectors. In India, Sahamati does the same for the banking and the healthcare sector. Both are producing governance rules and are working on concrete use cases to help build such human-centric data networks.

5 Levers of action

Having a clear regulatory environment will serve the users of data intermediary services, as they are safeguarded from risks associated with them.

5.1 For governments: Future-proof regulatory support

For entities to use and invest in data intermediaries, legal certainty is key. But this area is complex. Having a clear regulatory environment will serve the users of data intermediary services, as they are safeguarded from risks associated with them, and the flourishing of the market as a whole, as liability risks will be easier to navigate and competition will be rooted in a level playing field.

The demand is there: irrespective of regulatory gaps, more and more data trust initiatives are emerging because of their usefulness.[54]

The consensual sharing of data rests on the balance of incentives (such as for innovation, profit or philanthropy) and disincentives (such as privacy concerns and proprietary interests or other disincentives such as external regulatory intervention). In many cases, regulation intervenes to bridge this trust gap by demanding a level of data protection and privacy be adhered to. While that may tackle disincentives, in most markets there remains a lack of regulatory support for data sharing, although as mentioned earlier, this is shifting quickly.

In contrast, however, there usually is immense pressure on legislators to act in areas where existing data protection and privacy policy fails as a system, as in the case of high-profile data breaches. An example of this is AdTech and the constant opting in and out via cookie banners, where the European Parliament now calls for a complete ban of targeted advertisement in the European Union Digital Services Act.[55]

Effective trustworthy data intermediaries, which opt in or out on behalf of people, might ease the subjective need for strict legislation in specific industries and for specific use cases and instead allow for a more harmonized and holistic approach with multiple applications. The appeal of TDAs is that they are similarly simplistic and complex: when a TDA can navigate any data sharing scenario, the sky is the limit for the opportunity – and the risk.

BOX 6

Relevant existing and upcoming legislation

Prominent examples of existing or upcoming legislation concerning data intermediaries:

- **European Union GDPR**

  The European Union General Data Protection Regulation (GDPR)[56] lays down horizontally applicable rules on the handling of personal data in the European Union. It does not have explicit provisions on data intermediaries and could be amended to implement a clear and legally secure framework for them.

- **US ACCESS Act**

  In the United States, the ACCESS Act of 2019 is the first proposed federal legislation expressly allowing for end-users to delegate their data rights to trusted "third party custodians".[57] The proposed bill incorporates a general "duty of care" owed to the custodian's clients. Importantly, the proposal also requires that large platform companies provide these custodians with interconnection and data portability via transparent and accessible interfaces.[58] Such interoperability provisions will be key if trustworthy data intermediaries are to have a reasonable opportunity to fully represent the delegated interests of their clients and thereby compete successfully with large platform companies.

- **European Union Data Governance Act**

  Chapters 3 and 4 of the European Union Data Governance Act[59] discuss for-profit and not-for-profit data intermediaries at length. They comprise obligations such as that of neutrality of intermediaries and registration schemes, and establish the concept of data altruism and standardized consent forms.

Due to the risks that data intermediaries can pose to fundamental rights – next to their benefits if implemented correctly – it seems consequent to explore having certain provisions for data intermediaries enshrined in law.

- **Transparency and neutrality**

  Transparent data trusts may be more neutral than others. One way this can be achieved is by guaranteeing that the monetization of the service mainly derives from the management of the data and possibly the provision of added value services and not from using the data itself. The EU's Data Governance Act contains provisions of this nature and echoes the ePrivacy Directive[60] where providers of electronic communications services may transport data but may not harness it for their own purposes, including commercial use.

“ To move to a world of trusted digital agency, data portability must be explicitly supported in operational terms.

- **Data portability**

  Already provided for under data protection and privacy legislation, data portability is seldom supported in reality. To move to a world of trusted digital agency, data portability must be explicitly supported in operational terms. One way to manage data portability is via a data intermediary.

- **Fiduciary duty vs human-centricity**

  While imperfect, the fiduciary duties that are owed to the data subject could be defined in legislation, in particular in markets with no privacy and data protection law. An example of such a definition can again be found in the European Union Data Governance Act, which states that “the provider offering services to data subjects shall act in the data subjects’ best interest when facilitating the exercise of their rights, in particular by advising data subjects on potential data uses and standard terms and conditions attached to such uses”.[61] More generally, most privacy and data protection laws, such as the European Union GDPR, impose strict obligations on entities handling personal data, whether they act as a data controller or data processor. However, this may not be appropriate in all cases, especially where rights and interests collide or are unknown.

  Human-centricity is a more nuanced concept based on taking into account the interests of the person, their autonomy and their agency. Human-centric policies will help develop a human-centric data ecosystem within which human-centric data intermediaries can survive.

- **Insolvency**

  In instances where data is held directly by the data trust – and not decentralized and only managed centrally – provisions in cases of the entity’s insolvency or liquidation seem advisable.[62] This echoes well-understood security protocols and the decentralization of servers, as well as being the premise of decentralized autonomous organizations (DAOs).

- **Access rights of public authorities**

  Which and to what extent public authorities such as law enforcement and intelligence services shall have access to data managed by data intermediaries is naturally an area of conflict. This holds particularly true in cross-border cases, as can currently be observed in the ongoing US-European Union conflict over the Privacy Shield, which was recently struck down by the European Court of

“ It may be preferable to promote decentralized models (such as those in Web 3.0) that do not rely on a centralized database, or data sharing enabled by secure application programming interfaces that rely on strong authentication methodologies.

Justice because it deemed personal data not well enough protected from access from US intelligence.[63] Data retention and surveillance are usually matters of national security and defence; nevertheless, increased transparency increases trustworthiness in the data ecosystem.[64] For this reason it may be suggested that the intermediary enjoy a carve out requiring a warrant, much like telephone data in many jurisdictions.

- **Oversight**

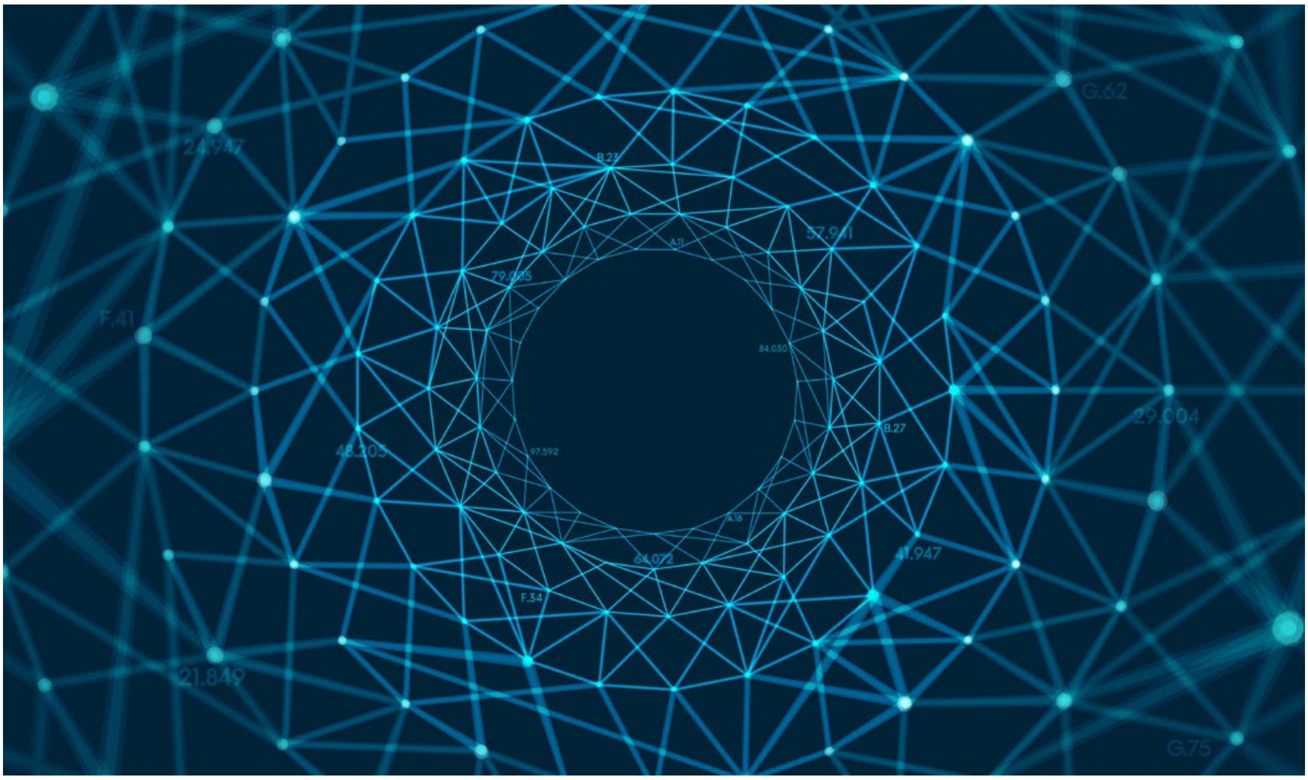
  As the inevitable counterpart of every legislative obligation, appropriate opportunities for oversight need to be guaranteed. This seems particularly reasonable in relation to data trusts, where certain risks such as unintended biases or discrimination would be hard to catch from the outside. Under current circumstances, that is likely to be a national regulator or data protection authority; but a new model could emerge, especially if fiduciary duty is required.

  Any regulatory framework with a weak regulator will not incentivize compliance, regardless of the intensity of the regulation. In addition, where a regulator also plays a more proactive role in publishing guidelines, best practice and standard templates, this will create additional trust in the knowledge that participants have a verified benchmarked to judge compliance. There is a balancing act to be struck and it could be that in those jurisdictions that have a weak regulator, the intermediary model will follow that same approach. The argument against this would be strengthening a data protection regulator, for example, to deal with data protection issues in relation to intermediaries, which increases the rights of the individual. But the business outcome argument to do this is more persuasive, as a stronger regulator, more trust in more sharing of data, and individual rights also increase. In addition, close collaboration among regulators – across countries and across sectors – would contribute to more effective enforcement and therefore further enhance trust in data sharing.

Recommendations for the development of standardized policies for data intermediaries:

- **Sandboxes** – It may be worth exploring how regulatory sandboxes can contribute to building trust in the data sharing economy. These sandboxes would enable data intermediaries and other participants to test new data sharing projects and technologies in a safe and controlled environment, while receiving privacy guidance.

- **Security** – Where data intermediaries get access to credentials (e.g. username and password) or amass vast amounts of personal data or confidential information, this raises potential security concerns. It may be preferable to promote decentralized models (such as those in Web 3.0) that do not rely on a centralized database, or data sharing enabled by secure application programming interfaces (APIs) that rely on strong authentication methodologies.



- **Liability:** Under certain limited circumstances it may be appropriate to establish a special regime for reduced liability for those entities that voluntarily accept the fiduciary duties of care, loyalty and confidentiality vis-à-vis their customers or patrons, and adhere to strict human-centric criteria. These entities would by design be required to go above and beyond current legal data protection and privacy requirements. Recognition of such a status could be geared to sector co- or self-regulatory measures, such as professional codes of conduct or best practices, which include robust enforcement measures to ensure compliance with the specified fiduciary duties. Such a regime would need to be tightly controlled to avoid the circumnavigation of the spirit of data protection and privacy laws and avoid unintended consequences.
- **Delegation:** Policy-makers may wish to consider developing a "right to delegate" provision in future data protection and privacy legislation. Such a provision is contained in the ACCESS Act legislation currently pending in the US Congress. To the extent that individuals are granted certain rights, such as data portability and interoperability, they also may also be granted express permission to delegate those rights to a trusted third party – a data intermediary. This mechanism would, among other things, prevent delay or interference with the ability of individual data subjects to exercise their rights with the assistance of trustworthy third parties. Such a provision could be limited to those entities that can satisfy specified pre-determined standards and would also need to be carefully monitored to avoid unintended consequences.

BOX 7

Cross-border data flows and data transfers

As a consequence of the GDPR's focus on the protection of the European Union's fundamental right to privacy, it contains a strict purpose limitation for granting consent, which currently hinders many use cases of data altruism. Another area with potential is that of cross-border data transfers: With the right amendments to the law, could an adequacy decision (Art. 45 GDPR) be issued in favour of a data trust?

Data intermediaries will need to consider where they are located, their place of legal establishment, corporate structure, and independence. They will also need to consider the impacts of legislative movements to localize the residency of data intermediaries and require representatives in-country, among other similar requirements, which could prejudice those use cases, even when ostensibly motivated to protect personal data.

Finally, it is critical to emphasize the need to enable and facilitate global data flows while maintaining high standards for privacy and security, as the free flow of data is the backbone of any data sharing economy.

5.2 For businesses: A policy leadership role

Meanwhile, as useful as regulation is, businesses also have a role to play in developing responsible data intermediaries. While some aspects of how business will ultimately drive the design of digital agents have already been discussed, responsible businesses may wish to explicitly consider the following:

– **Standards**

Widespread standards are a precondition for efficient and well-functioning data intermediary systems. Standardized machine-readable formats and communication protocols allow for the automation of the execution of services offered by data intermediaries and thus allow them to scale. The private sector has a crucial role to play in the adoption of standards: what industry as a whole uses ultimately becomes endorsed at a systemic level. A government, in turn, may endorse it later, either explicitly or implicitly; at the very least standards are passively tolerated.

– **Certification/licensing schemes**

Certification, or licensing schemes, such as certificates of conformity are a well-established co-regulatory measure and an acknowledged option for the regulation of data intermediaries.[65] A certification could work as follows: the legislation would define a set of core criteria that all certified intermediaries should meet in order to demonstrate their neutrality; this set of core criteria could be the absence of conflict of interest, no competition with data users (e.g. no development of own data apps in competition with others, so as to avoid any risks of self-preferencing) and the commitment to not discriminate between companies that would like to offer data services (openness obligation).[66] Certification under these criteria could then either be voluntary or compulsory.

– **Law enforcement and access requests**

This inevitable pressure to either resist or comply with lawful access or intelligence requests for data presents a host of challenges and implications, especially in light of three trends: (i) law enforcement and intelligence community responsibilities to safeguard national interests against domestic and transnational threats; (ii) increasing restrictions on cross-border data flows based in part on concerns with those lawful access/surveillance responsibilities and authorities; and (iii) increasing desire to localize and tap into data to develop revolutionary technologies like AI.

In addition, the fact that daily lives are increasingly lived online leads to requests between private parties to access data via mechanisms like a subpoena.

Businesses using data intermediaries will therefore need to consider:

- Whether to encrypt data in a way that only the authorized recipients can access the data – such that not even the intermediary itself can access the data in an intelligible fashion (which may, however, prevent the data intermediary from offering some services that require access to the data in the clear);
- Whether to seek legislative relief from and protection against lawful access requests; or
- Whether to create policies and procedures to handle such requests (which is a legal obligation under GDPR and other privacy laws globally).

– **Collaboration**

Finally, businesses may wish to consider learning from non-traditional allies, such as peers with different business models but who could benefit from the use of TDAs. Peer-to-peer learning can provide opportunities for the application of TDAs. Those applications in turn inform the broader policy and governance debate.

Conclusion

Opportunities abound to create and adopt novel solutions to the challenge of enabling users to make durable decisions for how data about them is used and to make sure their wishes are abided by – and to be able to share that data. Since it is not possible for every business to do this, the solution is to give them a service provider: a data intermediary. The idea of placing a trusted data intermediary inside the data value chain can also be a form of standardization. In order to fully harness the data ecosystem in a responsible, cohesive and interoperable manner, people, businesses and governments require trusted safeguards that respect human-centricity and proprietary rights alike when designing alternatives to notice and consent.

Businesses meanwhile are already using data intermediaries in instances of delegated agency, such as in the payments industry. Businesses are more empowered than they may believe given that digital agency policy is in its infancy; but it will become established in a way that endorses norms, including the identification and prevention of harms.

What could go wrong? What could go right?

In many ways, a lot of things are already going wrong. Users are carved up as products and their data used in ways they are uninformed about – or feel uninformed about; in ways that their data might be used, which could be inconsistent with the users' values or preferences; or in unexpected ways that the application did not disclose. In worst case scenarios, digital agents could lead to the non-transparent use of data, including in ways that harm the data subject.

At the system level, without efficient diversity, people may find the opposite – that they have or perceive to have reduced spectrum of choices or agency. This is due to the echo chamber effect of group think.

On the flip slide, a lot could go right:

- A balance of control for *any* user to understand the decision they are making as to voluntarily providing their data or withholding it, thanks to their understanding of the policy of the application and the accountability of the host company OR the scaling of the user's permission sets according to skill set on understanding technology.

- Granularity to provide options as to what data the user will volunteer (for example, if I am a dog owner, I might be happy to volunteer that data, so I get dog food ads; but I do not want my healthcare data shared).

- Improved data provenance as a result of increased legal certainty. It is essential to consider data provenance when working on things like blockchain and machine learning

- A user would have the ability to choose their preferred application, which might align with their personal values and the values of the application or company. An application may present choices to the user but the choices would already be created by the application.

- Some decision automation without interrupting the user's current task, without worrying about risky use of the data.

Trusted digital agency that harnesses the power of data intermediaries holds so much promise; but it is clear that a one-size-fits-all solution does not exist. Instead, it is necessary to look at lessons from industry and academia to observe what can be learned and the meaningful actions to take to successfully rewrite notice and consent where it is less relevant.

A multistakeholder call to action

In developing the rules of the game for trusted data intermediaries giving rise to a potentially automated regime of personal data sharing at a system level in a manner that overcomes the limitations of notice and consent regimes, it is the voice and presence of people that matter most. This presence can be amplified by taking a human-centric approach to the issue and placing people at the centre of such a step change in data policies.

But it also requires a multistakeholder approach to get right. It is only by listening – to people to understand their experience and desires, to businesses to understand their innovations and constraints, to scholars who can isolate commonalities between models, and of course to governments who aim for evidence-based policy-making from a unique vantage point – that it is possible to start to understand the rich tapestry of the implications of data intermediaries, especially trusted digital agents, in different scenarios.

The concept of trusted digital agency is effectively in policy "beta[67] mode and therefore requires testing from all stakeholders. Only when the concept is tested will it be possible to unearth the solutions that society will demand to advance towards trusted digital agency. That will be the key to holistic, systemic policy-making that leverages technological advancement for human-centric, pro-innovation purposes in areas such as international data transfers, healthcare research and diagnostics, innovation itself and a safer and more inclusive online world.

Glossary

Cross-border data flows
The movement of data across international borders, usually at the business-to-business level.

Data controller
As defined in the GDPR (Article 4), the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data ecosystem
The ecosystem within which data exists and operates, either locally or at a global level. This can include the data itself and the applications and infrastructure that support its storage, access, processing, use and reuse.

Data portability
The ability to port data from one system to another.

Data processing
As defined in the GDPR (Article 4), any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data processor
As defined in the GDPR (Article 4), a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.

Data protection and privacy laws
Laws that govern the collection and processing of personal data and personally identifiable information and that vary from territory to territory. These differences can act as both a hard and soft barrier to the movement of data across borders and can cover personal and/or non-personal data.

Data provenance
Identifies the origin of the data processor and data owner and documents a record of the history of the data since collection.

Data subject
As defined in the GDPR (Article 4), an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data trust
An entity or group of entities that is entrusted to manage a specific data ecosystem or data value chain.

Dataspace
A common space designated to use data for a specific purpose or purposes.

Decentralized autonomous organizations (DAOs)
Independent, self-governed and self-funded decentralized organizations based on a foundation of smart contracts.

ePrivacy Directive
Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

General Data Protection Regulation 2018 (GDPR)
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Human-centricity
Putting people's wants and needs at the forefront of process and systemic decision-making.

IoT (internet of things)
A network of items – each embedded with sensors – that are connected to the internet.

Metaverse
A virtual reality space in which users can interact with a computer-generated environment and other users.

Open Data Watch's Data Value Chain
The Data Value Chain framework[68] helps technical practitioners understand how interoperability adds value to data on the data value chain. The data value chain describes four major stages: collection, publication, uptake and impact. It is essential to reference interoperability at each stage, starting from when the handshake happens between systems, to either consume or deliver data in the value chain. For example, it will define classifications and standards to be followed while collecting and storing the data. Importantly, it describes how downstream systems should use the data. The interoperability checklist must also reflect the organizational practices and data management plans that cover the entire data value chain.

Open data
Data that is made available for anyone to access and use

Personal data
As defined in the GDPR (Article 4), any information relating to a data subject. It is important to note that information that relates to a data subject, even without a name, can qualify as personal data under the GDPR.

Regtech
First coined by the United Kingdom's Financial Conduct Authority (FCA) in 2015, which called it a "subset of fintech that focuses on technologies that may facilitate the delivery of regulatory requirements more efficiently and effectively than existing capabilities." In simple terms, it refers to any technology that ensures companies comply with their regulatory requirements.[69]

Software as a service (SaaS)
Software solutions that reside in the cloud but, due to high-speed connectivity, can be used in real time as if they resided locally.

User experience (UX) design
The design process through which people experience the technology they interact with.

Web 3.0 or Web 3
The third generation of the internet, which is decentralized in nature and enabled by distributed ledger technologies.

Zero-knowledge proof (ZKP)
A concept in cryptography whereby one party can prove the existence of something to another party without revealing the properties of that something.

Contributors

Lead author

Anne Josephine Flanagan
Data Policy and Governance Lead,
World Economic Forum

Task Force on Data Intermediaries (Co-authors)

Michael Bahar
Partner, Co-Lead, Global Cybersecurity and Data Privacy, Eversheds Sutherland

Paula Barrett
Partner, Co-Lead, Global Cybersecurity and Data Privacy, Eversheds Sutherland

Laura Brandimarte
Assistant Professor of Management Information Systems, University of Arizona

Matthias De Bievre
Chief Executive Officer, VISIONS

Megan Doerr
Principal Scientist, Sage Bionetworks

Edwin Doyle
Global Security Strategist, Check Point Software

Cristian I. Duda
Managing Partner, Chief Digital Officer,
Haefeli & Schroeder Financial Lines

Richard Gomer
Research Fellow, Trust & Digital Agency,
University of Southampton

Jana Gooth
Legal Policy Adviser, European Parliament

Jennifer King
Privacy and Data Policy Fellow, Stanford Institute for Human-Centered Artificial Intelligence

Gary LaFever
Chief Executive Officer, Anonos

Xiao Liu
Assistant Professor, McGill University

Caroline Louveaux
Chief Privacy Officer, Mastercard

Ewa Luger
Chancellor's Fellow, The Alan Turing Institute,
Edinburgh University

Bijan Madhani
Privacy and Data Policy Lead, Meta

Allan Millington
Director, Data Office, EY

Teresa Patraquim da Conceição
Head Privacy Team, International, Novartis

Steven Tiell
Lead, Responsible Innovation + Data Ethics,
Accenture

Aleksandr Tiulkanov
Special Adviser on Digital Development,
Council of Europe

Joe Toscano
Founder, BEACON

Stefaan Verhulst
Co-Founder and Chief Research and Development Officer, Governance Lab @ NYU

Jacques de Werra
Professor of Law; Director, Digital Law Center,
University of Geneva

Richard Whitt
President, GLIA Foundation; Founder and Chief Executive Officer, Deeper Edge

Christian Wickert
Head, New Technologies Policy, USA, Merck

Acknowledgements

Suzie Albizzati
Head, Corporate Marketing, AlixPartners

Donald Bullers
Global Technical Lead, Elastos Foundation

Jan Huizeling
Vice-President, Digital Labs, Yara International

Robert Kain
Chief Executive Officer and Co-Founder, LunaPBC

Richard Kibble
Global Head, Data Privacy, Alcon

Morgan Livingston
Science Policy Fellow, IDA Science and Technology Policy Institute

World Economic Forum

Kimmy Bettinger
Project Specialist, Data Policy

Evîn Cheikosman
Policy Analyst, Crypto Impact and Sustainability Accelerator

Tenzin Chomphel
Project Coordinator, Data Policy

Sheila Warren
Deputy Head, Centre for the Fourth Industrial Revolution Network

Danielle Carpenter
Editor

Laurence Denmark
Design

Endnotes

1. World Economic Forum, 2020, *Redesigning Data Privacy: Reimagining Notice & Consent for human-technology interaction*, https://www.weforum.org/reports/redesigning-data-privacy-reimagining-notice-consent-for-humantechnology-interaction.
2. Ibid.
3. McDermott, B., 2019, “Mind The Gap: The Trust/Experience Paradox”, *Forbes*, https://www.forbes.com/sites/sap/2019/01/15/mind-the-gap-the-trustexperience-paradox/?sh=4df2fd4e6275.
4. Hardin, R., 2002, Trust and Trustworthiness, Russell Sage Foundation.
5. World Economic Forum, 2020, *Redesigning Data Privacy: Reimagining Notice & Consent for human-technology interaction*, https://www.weforum.org/reports/redesigning-data-privacy-reimagining-notice-consent-for-humantechnology-interaction.
6. Tierney, J., 2011, “Do you suffer from decision fatigue?”, *New York Times,* https://www.nytimes.com/2011/08/21/magazine/do-you-suffer-from-decision-fatigue.html.
7. McDonald, A.M and Cranor, L.F., 2008, “The Cost of Reading Privacy Policies”, *I/S: A Journal of Law and Policy for the Information Society*, 2008 Privacy Year in Review issue.
8. Data2X and Open Data Watch, n.d., *The Data Value Chain: Moving from Production to Impact*, https://opendatawatch.com/wp-content/uploads/2018/03/Data_Value_Chain-WR-1803126.pdf.
9. GDPR Article 4 requires heightened requirements for pseudonymisation beyond merely replacing direct identifiers with tokens for individual fields within a single data set. Such heightened requirements for pseudonymization include protecting all data elements, protecting against singling out attacks, dynamism, non-algorithmic lookup tables and controlled re-linkability,
10. World Economic Forum, 2019, *Federated Data Systems: Balancing Innovation and Trust in the Use of Sensitive Data*, https://www3.weforum.org/docs/WEF_Federated_Data_Systems_2019.pdf.
11. World Economic Forum, 2021, *Empowered Data Societies: A Human-Centric Approach to Data Relationships*, https://www3.weforum.org/docs/WEF_Empowered_Data_Societies_2021.pdf.
12. European Commission, 2020, Data sharing in the EU – common European data spaces (new rules), https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12491-Data-sharing-in-the-EU-common-European-data-spaces-new-rules-_en\.
13. Tiel, Steven, 2020, “AI Ethics vs Data Ethics”, Ethics of Data, https://ethicsofdata.com/ai-ethics-vs-data-ethics.
14. Data2X and Open Data Watch, n.d., *The Data Value Chain: Moving from Production to Impact*, https://opendatawatch.com/wp-content/uploads/2018/03/Data_Value_Chain-WR-1803126.pdf.
15. Corritore, C. L., Kracher, B., & Wiedenbeck, S., 2003, “On-line trust: concepts, evolving themes, a model”, *International Journal of Human-Computer Studies*, 58(6):737–758, 2003.
16. Ibid.
17. Kapoor, A. & Whitt, R.S. 2021, *Nudging Towards Data Equity: The Role of Stewardship and Fiduciaries in the Digital Economy*.
18. Ibid.
19. Verhulst, S.G., 2021, “Reimagining Data Responsibility: 10 new approaches toward a culture of trust in in re-using data to address critical public needs”, *Data & Policy*, 3, 2021.
20. Whitt, Richard S., 2020, “Old School Goes Online: Exploring Fiduciary Obligations of Loyalty and Care in the Digital Platforms Era”, 36 *Santa Clara High Tech. L.J.* 75, https://digitalcommons.law.scu.edu/chtlj/vol36/iss1/3.
21. Brandusescu, A. & van Geuns, J., 2020, *Shifting Power through Data Governance 2020*, https://assets.mofoprod.net/network/documents/ShiftingPower.pdf.
22. Delacroix, S. & Lawrence, N.D., 2019, “Bottom-up data Trusts: disturbing the ‘one size fits all’ approach to data governance”, *International Data Privacy Law,* vol. 9, issue 4, November 2019.
23. Cohen, C. and Wendehorst, C., 2021, ALI-ELI Principles for a Data Economy, Data Transactions and Data Rights, ELI Final Council Draft, https://www.principlesforadataeconomy.org/.
24. Young, A. & Verhulst, S.G., 2020, “Data collaboratives”. In: Harris, P, Bitonti, A, Fleisher, C, Skorkjær, BA (eds) *The Palgrave Encyclopedia of Interest Groups, Lobbying and Public Affairs*. Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-030-13895-0_92-1.Google Scholar
25. Ada Lovelace Institute, 2021, Exploring Legal Mechanisms for Data Stewardship, https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/.
26. Ibid.

27. Ostrom, E., 2015, *Governing the Commons: The Evolution of Institutions for Collective Action*, Cambridge University Press.

28. Ada Lovelace Institute, 2021, Exploring Legal Mechanisms for Data Stewardship, https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/.

29. Some entities are experimenting with various real-world proof of concept exercises to determine, among other factors, the potential viability and scalability of the commercial digital fiduciary model. See Whitt, R., 2021, *Gaining Real-World Validation of the Digital Fiduciary Model*, Aapti Institute, The Data Economy Lab, White Paper Series, November 2021, https://www.linkedin.com/feed/update/urn:li:activity:6874905018835849216/.

30. European Parliament, 2020, Regulation of the European Parliament and of the Council on European data governance COM(2020) 767 final.

31. H.M. Government, 2021, *Unlocking the value of data: Exploring the role of data intermediaries*, https://www.gov.uk/government/publications/unlocking-the-value-of-data-exploring-the-role-of-data-intermediaries/unlocking-the-value-of-data-exploring-the-role-of-data-intermediaries.

32. Lähteenoja, V., Flanagan, A. J., & Warren, S., 2021, "On the importance of human-centricity and data", World Economic Forum, https://www3.weforum.org/docs/WEF_On_the_Importance_of_Human_Centricity_2021.pdf.

33. Other fiduciary duties include good faith and confidentiality, as per *Black's Law Dictionary*, 2019, 11th ed. which defines other fiduciary duties as "good faith, trust, special confidence, and candor".

34. Lähteenoja, V., Flanagan, A. J., & Warren, S., 2021, "On the importance of human-centricity and data", World Economic Forum, https://www3.weforum.org/docs/WEF_On_the_Importance_of_Human_Centricity_2021.pdf.

35. See Open Data Institute, 2019, *Data trusts: legal and governance considerations*, https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf, p. 8: "court action is expensive and likely to be too slow for the needs of a data trust, which include maintaining confidence that its rules provide appropriate protections for all the stakeholders in data. Thus, the report suggests that alternative dispute resolution mechanisms need to be incorporated into the data trust's rules".

36. On the emergence of data disputes and of data arbitration, see de Werra, J., 2019, "Using Arbitration and ADR for Disputes about Personal and Non-Personal Data: What Lessons from Recent Developments in Europe?", *American Review of International Arbitration*, vol. 30, n° 2, p. 195-217, available at: https://archive-ouverte.unige.ch/unige:134313; de Werra, J., 2018, "From Intellectual Property (Data-Related) Disputes to Data Disputes: Towards the Creation of a Global Dispute Resolution Ecosystem for Data Disputes in the Digital Era", in: *Resolving IP Disputes* (Graz: NWV Verlag), 2018, p. 87-109, available at: https://archive-ouverte.unige.ch/unige:113027.

37. de Werra, J., 2016, "ADR in Cyberspace: The Need to Adopt Global Alternative Dispute Resolution Mechanisms for Addressing the Challenges of Massive Online Micro-Justice"*, Swiss Review of International & European Law* 2016, 289-306, https://ssrn.com/abstract=2783213.

38. See the report *Data trusts: legal and governance considerations* by BPE Solicitors, Pinsent Masons and Chris Reed at Queen Mary University of London, 2019, https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf, p. 8: "[…] court action is expensive and likely to be too slow for the needs of a data trust, which include maintaining confidence that its rules provide appropriate protections for all the stakeholders in data. Thus the report suggests that alternative dispute resolution mechanisms need to be incorporated into the data trust's rules."

    See also de Werra, J., 2016, "ADR in Cyberspace: The Need to Adopt Global Alternative Dispute Resolution Mechanisms for Addressing the Challenges of Massive Online Micro-Justice", *Swiss Review of International & European Law* 2016, 289-306, https://ssrn.com/abstract=2783213.

39. See the report *Data trusts: legal and governance considerations* by BPE Solicitors, Pinsent Masons and Chris Reed at Queen Mary University of London, 2019, https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf, p. 41: "[…] dispute review boards ("DRB"), are ordinarily seen under construction contracts and exist for the length of a particular project. These are put in place by contractual arrangement and governed by the International Chamber of Commerce Board Rules. The model however could equally be applicable to disputes arising out of a data trust if similar DRB provisions were to be put into the terms of use for the providing or licensing of data."

40. International Network on Digital Self-Determination, https://idsd.network/.

41. Source: World Economic Forum, 2018, *Identity in a Digital World: A new chapter in the social contract*, https://www.weforum.org/reports/identity-in-a-digital-world-a-new-chapter-in-the-social-contract.

42. World Economic Forum, 2018, *Identity in a Digital World: A new chapter in the social contract*, https://www.weforum.org/reports/identity-in-a-digital-world-a-new-chapter-in-the-social-contract.

43. Kinston, J. & Ng, I., 2021, "Personal Data Servers will help take back digital ID from big tech", *Wired*, https://www.wired.co.uk/article/personal-data-servers.

44. Centre for Data Ethics and Innovation, 2021, *Unlocking the value of data: Exploring the role of data intermediaries – An exploration of the role intermediaries could play in supporting responsible data sharing*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004925/Data_intermediaries_-_accessible_version.pdf.

45. Turner, C., David, S., Ahuja, A. & Wulfsohn, G., 2016, *Accenture Labs Ethical algorithms for "sense and respond" systems*, Accenture, https://www.academia.edu/31436602/Accenture_Labs_Ethical_algorithms_for_sense_and_respond_systems.

46. Future of Privacy Forum, 2017, *Unfairness By Algorithm: Distilling the Harms of Automated Decision-Making*, https://fpf.org/wp-content/uploads/2017/12/FPF-Automated-Decision-Making-Harms-and-Mitigation-Charts.pdf.

47. For example, see Jennings, N. & Wooldridge, W., 1996, "Software Agents", *IEE Review*, January 1996, pp 17-20, *http://www.cs.ox.ac.uk/people/michael.wooldridge/pubs/iee-review96.pdf*.

48. Ibid.

49. Friedman, B., Smith, I., Kahn, P., Consolvo, S., Selawski, J., 2006, "Development of a Privacy Addendum for Open-Source Licenses: Value Sensitive Design in Industry", *Proc. UBICOMP*, ACM Press (2006) 194—211.

50. Luger, E. & Rodden, T., 2013, "An Informed View on Consent for Ubicomp". *UbiComp '13: Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing*, September 2013, pp. 529–538, https://doi.org/10.1145/2493432.2493446.

51. Human Data Interaction, n.d., What is Human-Data Interaction?, https://hdi-network.org/intro_to_hdi/.

52. Diver, L., 2020, "Computational Legalism and the Affordance of Delay in Law", *Journal of Cross-Disciplinary Research in Computational Law* 1 (1), https://journalcrcl.org/crcl/article/view/3.

53. Luger, E. & Rodden, T., 2013, "An Informed View on Consent for Ubicomp". *UbiComp '13: Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing*, September 2013, pp. 529–538, https://doi.org/10.1145/2493432.2493446.

54. See for example:

- MyData Operators, which is empower individuals by improving their right to self-determination regarding their personal data, at https://mydata.org/;
- Decode, a consortium of 15 organizations from across the European Union, at https://www.decodeproject.eu/;
- The Solid project at the Massachusetts Institute of Technology, at https://solid.mit.edu/;
- RadicalxChange (RxC), a global movement for next-generation political economies, at https://radicalxchange.org/.

55. European Parliament resolution of 20 October 2020 with recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online (2020/2019(INL)), Art. 17, https://www.europarl.europa.eu/doceo/document/TA-9-2020-0273_EN.html.

56. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj.

57. See Whitt, R., 2021, "Hacking the SEAMs: Elevating Digital Autonomy and Agency for Humans", *Colorado Technology Law Journal*, Vol. 19, Issue 1, 137, 202 (2021).

58. Ibid.

59. European Parliament, 2020, Regulation of the European Parliament and of the Council on European data governance COM (2020) 767.

60. European Parliament and European Council, 2002, Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) as amended, https://eur-lex.europa.eu/eli/dir/2002/58/oj.

61. European Parliament, 2020, Regulation of the European Parliament and of the Council on European data governance COM (2020) 767 final.

62. Cf. Data Ethics Commission of the Federal Government of Germany, 2019, *Opinion of the Data Ethics Commission*, p. 134, https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN_lang.pdf?__blob=publicationFile&v=3.

63. InfoCuria, n.d., Case-law, https://curia.europa.eu/juris/documents.jsf?num=C-311/18.

64. World Economic Forum, 2021, *A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy*, https://www.weforum.org/whitepapers/a-roadmap-for-crossborder-data-flows-future-proofing-readiness-and-cooperation-in-the-new-data-economy.

65. European Parliament, 2020, Regulation of the European Parliament and of the Council on European data governance COM (2020) 767.

66. European Commission, 2020, EU Commission impact assessment accompanying the proposal for a Regulation on data governance (Data Governance Act) from 25 November 2020, SWD (2020) 295 final, p. 26, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=71225.

67. Beta mode is the test and trial period for a new piece of software when rapid learning and experimentation occur.

68. Open Data Watch, 2018, "The Data Value Chain: Moving from Production to Impact", https://opendatawatch.com/publications/the-data-value-chain-moving-from-production-to-impact/.

69. EQS Group, 2021, "What Is RegTech?", https://www.eqs.com/en-us/compliance-knowledge/blog/what-is-regtech/.

WORLD
ECONOMIC
FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org