WORLD ECONOMIC FORUM

Data for Common Purpose: Leveraging Consent to Build Trust

WHITE PAPER

NOVEMBER 2021

Images: Getty Images

Contents

Foreword

There are important opportunities to improve permissioning and consent management experiences in data exchanges for the common good.

Shelia Warren
Deputy Head of the Centre for the Fourth Industrial Revolution, Member of the Executive Committee, World Economic Forum

Bob Hedges
Senior Vice-President, Global Strategic Initiatives, Visa

In recent years, the world has experienced an exponential increase in the amount of data being generated, collected, stored and used. In addition, the context in which consumers manage any decision-making regarding the use of their data has significantly evolved. Public scepticism of corporate practices relating to the use of consumer data has been fuelled by high-profile cases of questionable conduct. At the same time, the challenges of the COVID-19 economic recovery, equitable energy distribution and climate change have provided excellent examples of how, if properly managed, consumer data can be very effectively shared and used for public benefit.

While the context for decision-making on data sharing has evolved to reflect new use cases and consumer preferences, the required infrastructure investment has not kept pace with this seismic shift in the data landscape. Making consumer-permissioned data sharing work has emerged as a major implementation challenge. Cross-border data-sharing interoperability has also been spotlighted as a critical need.

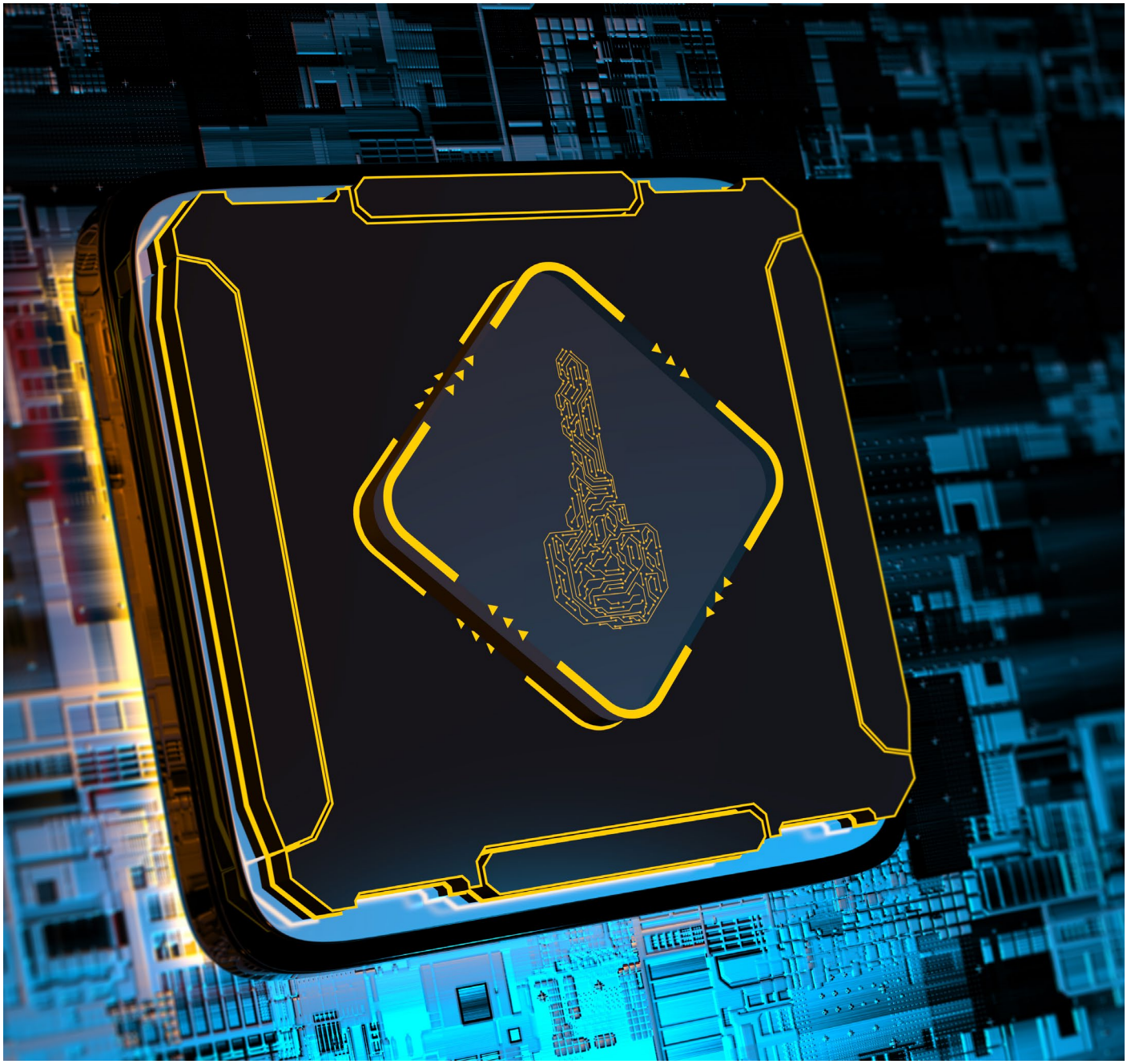
To fully support individuals' decision-making regarding the use of their data, the ecosystem needs to evolve towards a more global and consistent framework for data permissioning.

Alongside recognizing the need to empower consumers to manage their data effectively comes the realization that doing so requires common practices and protocols regarding how data sharing should be managed. While there are laws governing how businesses use data, those same laws provide only limited, if any, empowerment or guidance in terms of how to facilitate informed consumer choices. With no global framework to consistently define individuals' data rights, it is not surprising that little infrastructure investment has been made to clarify and bolster consumers' data choices. In contrast, for example, consider how the food nutrition label is now one of the most widely recognized standardized graphics in the world, allowing consumers to evaluate their food selection decisions. There is no equivalent format for data permissions to formalize, standardize and support individuals' decision-making about their data.

By more formally defining the data rights of individuals, recent regulations have spawned a wave of new technologies and practices aimed at arming consumers with greater data empowerment and control. Governments, financial institutions and large corporates are now proactively exploring how best to define and develop an "empowered" data permissions experience for individuals. These experiences seek to address the new regulatory requirements on data rights as well as achieve a higher level of consumer confidence in data sharing and digital commerce more broadly. Globally, tech start-ups, venture funds, public-sector agencies and research institutions are now working to deliver solutions for data permissioning that support consumers and drive higher consumer confidence and engagement in data sharing and digital commerce.

Considering the many developments around the world and across industries, there are important opportunities for progress to be made in terms of creating permissioning and consent-management experiences that pragmatically balance: (a) enabling individuals to make informed decisions about sharing their data; and (b) ensuring the seamless, efficient, scalable and interoperable permissioning of data. By investing in the development of the required foundations, we can expect a more mature and productive data-sharing process to replace today's underdeveloped, fragmented and inconsistent approach to consumer data permissions.

Through active engagement with leading stakeholders in the data-sharing ecosystem, the Data for a Common Purpose Initiative (DCPI) seeks to design and pilot data-sharing governance solutions that support the development of more mature processes and build consumer trust through consent management and permissioning for individuals' data.



Executive summary

An individual empowering approach is needed in permissions and consent management.

Trust in data sharing is broken

Individuals are becoming more and more aware of the misuse of data in the digital ecosystem. Data breaches are on the rise, data is being used without explicit consent and "dark patterns" are misleading individuals on why they are sharing their data. These experiences are far too common, creating uncertainty and mistrust.

Thoughtfully designed permissions and consent experiences can rebuild trust

Clear, consistent and granular permissions and consent models – aimed at educating and giving control back to the individual – can strengthen trust and maximize data sharing for the common good. As part of the Data for a Common Purpose Initiative (DCPI), along with multistakeholder input, this paper introduces how different attributes that build trust can be represented through consent mechanisms.

Consideration needs to be given to the commercial, governance and technological aspects of data permissions and consent

Within a data marketplace, there are three pillars of operations that support consent. The first, *commercial* actions, considers an individual's interaction points with consent choices (e.g. user experience). The second, *governance* mechanisms, includes the internal rules and processes that support consent choices. Finally, *technology* examines the elements that enable both the established interaction points and the governance aspects of individuals' permissions and consent experiences.

It is important to build trust attributes into consent mechanisms for data exchanges

Within the context of permissions and consent, trust is enabled through attributes encompassed within four groups: data exchange accountability, data protection, individual understanding and individual control. Reflecting these attributes in an individual's data permissions and consent experience can instil trust and maximize data sharing. A description of each attribute is shared in this paper; further details on how to operationalize these attributes will be published in a Consent and Trust Toolkit during the first quarter of 2022.

Introduction: Trust erosion in data sharing

Taking care not to repeat the data misuse mistakes of the past will play a key role in the success of data exchanges.

Trust is strongly recognized when it is being broken and lost.[1]

Trust in the use of data has been eroded over the past few years as more and more companies have been publicly exposed for their unethical collection, use or sharing of data. At the end of the third quarter of 2021, *Forbes* reported an Identity Theft Research Center study that showed the world had already seen 17% more data breaches in 2021 than in all four quarters of 2020 – 1,291 as against 1,018.[2] In other cases, data is collected, used and shared without a clear purpose or without explicit consent from the individual. The most famous example is the Facebook and Cambridge Analytica scandal, where Cambridge Analytica collected personally identifiable data from millions of Facebook users without their consent and then allegedly used that data to influence the 2016 US presidential election.[3] The US Federal Trade Commission voted unanimously to call the company's practices deceptive.[4] More recently, journalists have been exposing companies for their "dark-pattern" behaviour. According to the California Privacy Rights Act, a dark pattern is "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice".[5]

Examples of dark patterns encountered in applications that individuals use every day include, but are not limited to:

- Burying the terms of data use in complex privacy notices
- Using deliberately hard-to-understand language to discourage individual action
- Designing account closure processes that hinder or prevent individuals from deleting their previously shared account information and data
- Developing hidden, parallel profiles of individuals with additional personal data of which they are unaware
- Making it easy for individuals to consent to the storing and processing of their data, but making it difficult to withdraw their consent[6]

Though not all illegal, these patterns play to the commercial interests of private-sector data holders and hinder the ability of individuals to effectively manage and control the use of their data. When exposed to these tactics, they become less trustful of the company asking for data, as well as the digital economy as a whole. According to Visa's Data Privacy Study, in some major markets more than 90% of individuals are at least "somewhat concerned" about the privacy of the data they share online.[7] To instil trust in data sharing, it is pivotal to design data-sharing experiences that put the control back in individuals' hands.

As part of the multiyear Data for a Common Purpose Initiative (DCPI), this paper will be the first of multiple deliverables on the topic of consent and trust as it applies to data exchanges. The paper aims to establish a framework to design consent mechanisms that inspire trust in data exchanges. Subsequent toolkits and pilot programmes will examine design considerations for the framework, including key questions, implementation options and live tests.

Data for a Common Purpose Initiative (DCPI)

Launched in 2020, the Data for a Common Purpose Initiative (DCPI) aims to find ways to link, connect and exchange data assets for the common good, while protecting individual parties' rights and ensuring the equitable allocation of risks and rewards. Meeting this goal will require the creation of new and flexible data-governance models that support the combination and exchange of data from various origins, including personal, commercial and/or government sources. The World Economic Forum's white paper *Data-Driven Economies: Foundations for Our Common Future*, published in April 2021, describes the DCPI vision.

Accelerating the responsible exchange and use of data can solve critical challenges and fuel innovation for society. The DCPI supports the theory that leveraging data for the benefit of society involves five requirements:

Leveraging data for better outcomes

Connects contributors and consumers of data through data exchanges and marketplaces

Supports collaboration with data from personal, commercial and/or government sources, grounded in ethical use and always respecting rights

Unlocks data by decoupling the source from the purpose, with data used for multiple purposes across both the commercial and public sectors

Recognizes the rights of all stakeholders and allocates both the economic benefits and risks to all

Harnesses Fourth Industrial Revolution technologies

In addition to building upon the DCPI vision, the issue of building trust for the sharing of data was previously explored in the Forum's work *Redesigning Data Privacy: Reimagining Notice and Consent for Human Technology Interaction*, which highlights the importance of context and the appropriateness (or otherwise) of formal "notice and consent" approaches. The report frames the decision-making variables of a person consenting to share data about themselves, their behaviour or the type of technical device being used. For those occasions when notice and consent is the most appropriate means of data collection and use, businesses have an opportunity to improve privacy norms for the collection and processing of personal data. This paper, focused on trust and consent, is designed to bridge the gap between public expectations and the DCPI's vision of multistakeholder data exchanges where personal data can be used for common-purpose outcomes in a human-centred, privacy-adhering and trustworthy manner.

1 Creating trust through consent mechanisms in data exchanges

User experience, governance and technical architecture are key to supporting interoperability and future global ubiquity.

BOX 1 | **Key terms defined**

This key term, which may have different meaning in other contexts, will be referenced throughout this paper with the following definition.

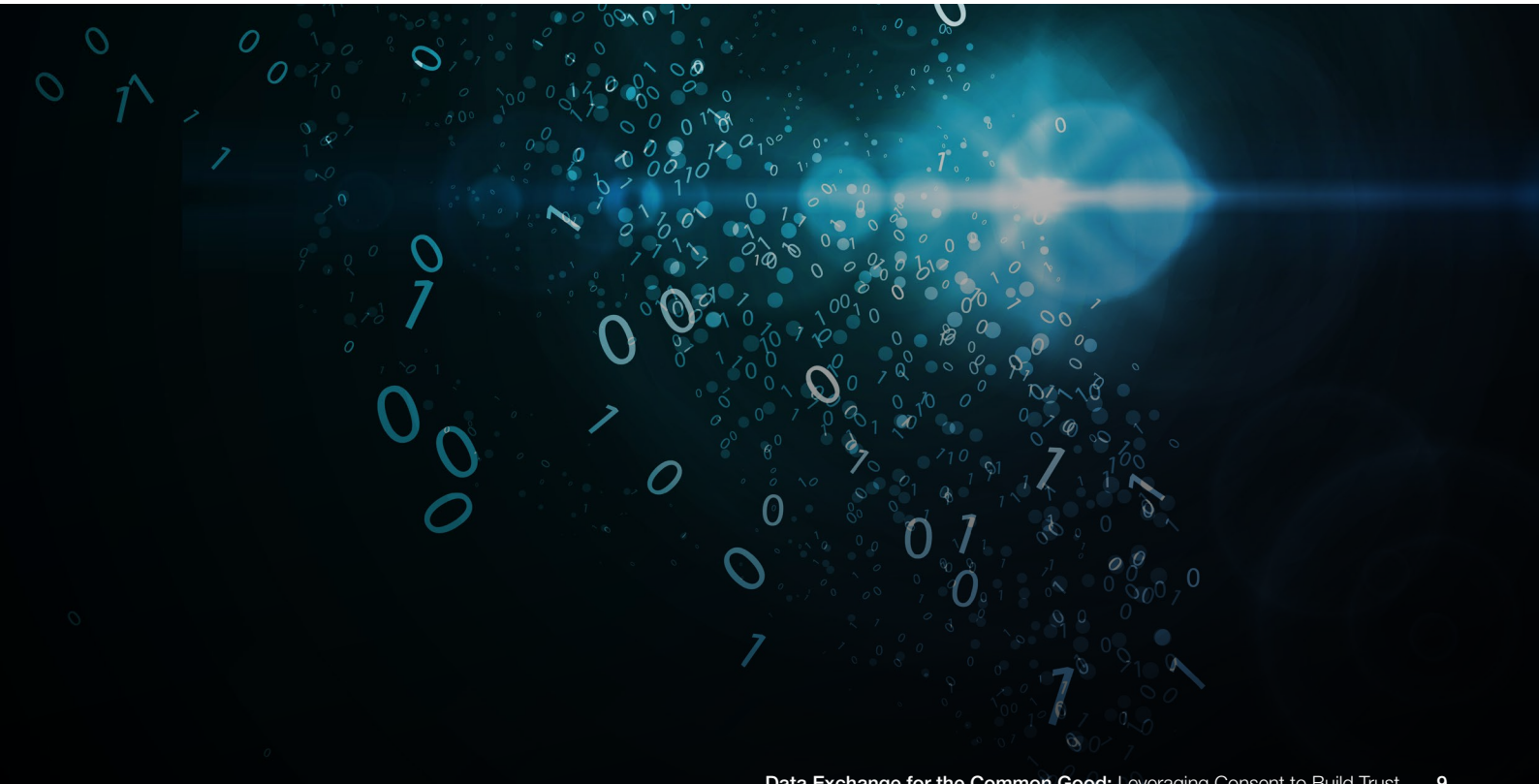
Person, individual or user
Referred to as a "person", "individual" or "user" throughout the paper, a single person, whose data may be collected, used or shared through a data exchange

> Charting a new course that supports both privacy and data sharing has one primary requirement – trust of the individual.

The global market for data has reached a crossroads. On one side, individuals' data must be protected: kept safe and private. On the other, the power of sharing data is unmistakable: it supports the private and public sectors in innovating to create a better world. While opportunities for good exist, individuals' perception of benefits distribution is also clear; according to Visa's Consumer Empowerment study, 68% of consumes believe companies benefit more from using their data than they do.[8] While these two paths of privacy and sharing have distinct priorities and obligations, they do not have to be mutually exclusive and there are ways to support both, simultaneously. Charting a new course that supports both privacy and data sharing has one primary requirement – trust of the individual.

The complexity of the personal data ecosystem is vast, and there are many challenges associated with strengthening trust in data sharing, even in support of the common good. There are increasing volumes of passively generated "observational" non-personal data that has an increasing impact on the lives of individuals, which is outside of the scope of this framework. Likewise, the paper focuses on the user-interface/user-experience layer and how to maximize those elements to educate and enable individuals to make meaningful choices. Also highly relevant (and to be covered in more detail in upcoming World Economic Forum publications) are innovations for strengthening trust with individuals via privacy-enhancing technologies (PETs), network infrastructure, data-management solutions and system architectures.

This paper, focused on improving trust through consent mechanisms, also recognizes the need for commercial and technology stakeholders to align on more trustworthy and human-centred business models in which the trust, consent and active engagement of individuals is foundational. These approaches stand in contrast to the current use of data exhaust (i.e. the trail of data left by the activities of individuals interacting with digital systems such as the internet or digital hardware, e.g. a mobile device) and derivatives for downstream purposes outside of the originally collected context. This concept of using data for secondary purposes without explicit consent is what Harvard professor Shoshana Zuboff famously defined as "surveillance capitalism, the unilateral claiming of private human experience as free raw material for translation into behavioural data. [This data is] then computed and packaged as prediction products and sold into behavioral futures markets – business customers with a commercial interest in knowing what we will do now, soon and later."[9]



BOX 2 | **Key terms defined**

These key terms, which may have different meaning in other contexts, will be referenced throughout this paper with the following definitions.

Consent mechanisms
The experience an individual has when giving permission for their data to be collected, used or shared in a data exchange

Data exchange (DEx)
Facilitates the exchange of data between participants in a trusted, legally compliant environment

Participants
Organizations, public or private, that collect, share or store data in a data exchange

Data exchanges for the common good
These allow data to be used for broader sets of social outcomes than is currently possible through most existing data platforms, and support the combination and exchange of data from multiple origins (e.g. personal, commercial or government sources)

Operator
The organization responsible for establishing and managing the operations of a data exchange

A utopian outcome would be for all individuals whose data is collected, used or shared in a data exchange for the common good to be directly aware of any data transaction and cognisant that sensitive or personal data is being generated and could be accessed by multiple entities. Individuals would have the ability to make informed choices and have transparency as to where their data goes beyond the entity seeking the individual's permission, and the integrity of the original context of the individual's permissioning choices would be maintained. While there are many hurdles to reaching such a utopia, this paper aims to support data exchange stakeholders to achieve more idealistic outcomes in the short term and create the conditions for more global ubiquity in the future.

Consent mechanisms are vital for strengthening trust. By gathering permissions, they are the first and primary **data exchange (DEx)** interaction point between individuals, **participants** and **data exchanges for the common good.**

As data exchanges for the common good are established around the world, **operators** should take a thoughtful approach in considering how design decisions will ultimately strengthen trust and positively affect the experiences of individuals who contribute data.

1.1 Scope of work for the DCPI's Consent and Trust Framework

While there are many options for establishing trustworthy data exchanges, this workstream is focused on how to do so through innovative consent mechanisms. For the purposes of this framework, it is assumed that the data exchange is a "secure" platform. Further trust drivers (e.g. identity verification, security measures) are also relevant but not currently addressed within this workstream.

2 Why do we need a framework for consent and trust in data exchanges?

Traditional models of notice and consent are no longer sufficient.

BOX 3 | **Key terms defined**

These key terms, which may have different meaning in other contexts, will be referenced throughout this paper with the following definitions.

Non-personal data
Data that cannot be directly or indirectly linked to an identified or identifiable natural person

Personal data
Data relating to an identified or identifiable natural person

Data of personal origin
Data that originates from an individual

Explicit consent
An individual has given a clear, unambiguous agreement for their data to be used for a specific purpose

> In today's world, policy and technology move at different speeds – while user experiences fall short.

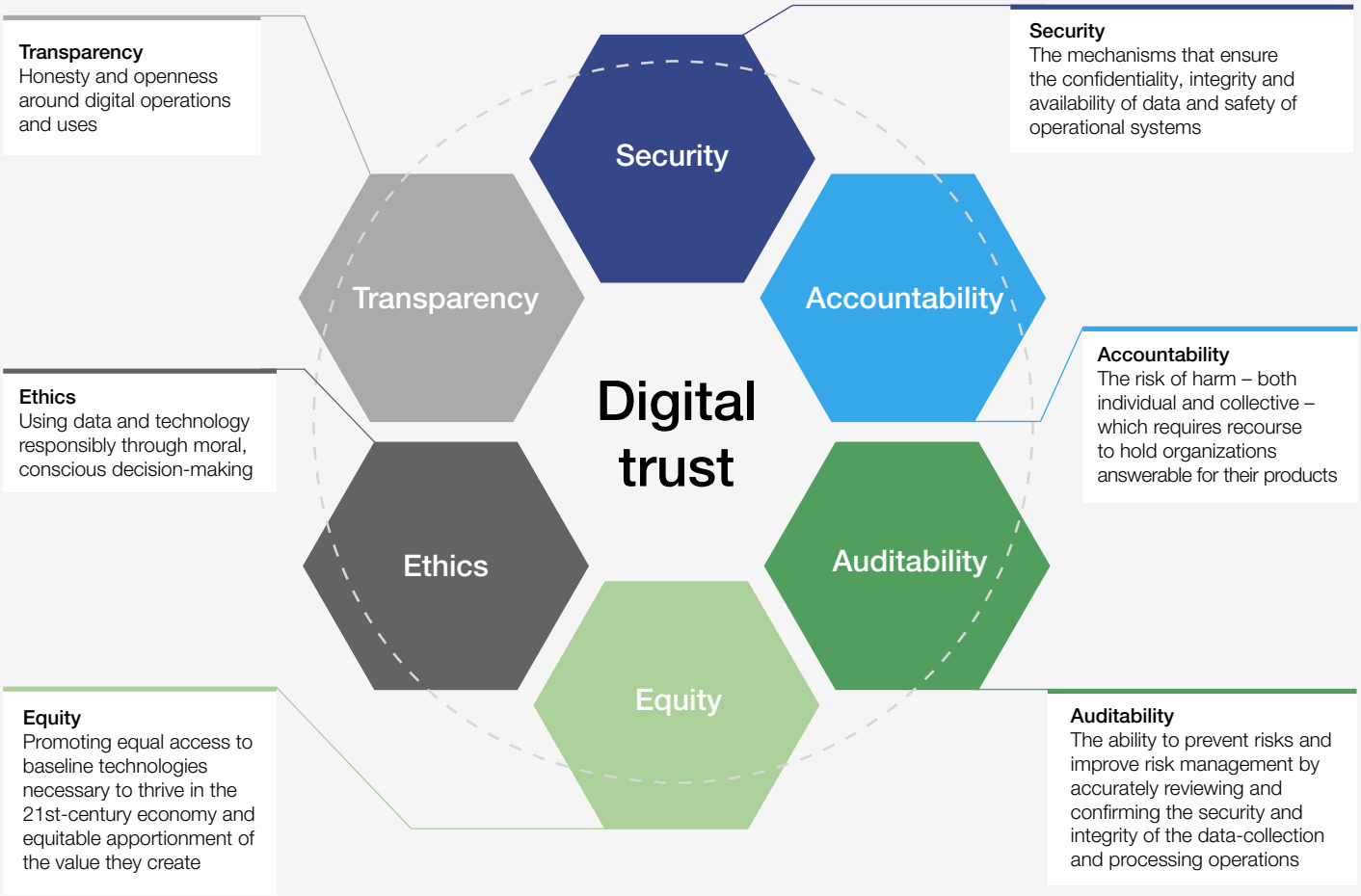
Data exchanges are designed to either ingest or catalogue available data from many different sources. Some of this data will have no direct connection to an individual and may not require an individual's consent to be collected, used or shared; this type of data is known as **non-personal data** (e.g. oceanic data recording sea levels and water temperature). However, in many cases the data will be **personal data** or **data of personal origin** – in these cases, even if personal identifiers are removed, individuals may still need to provide **explicit consent** for their data to be collected, used and/or shared. According to Visa's Consumer Empowerment Study, 76% of individuals want to take more direct control or have the option to have more control over their data, rather than companies and governments doing a better job of managing their data on their behalf.[10]

Traditional models of notice and consent are no longer sufficient as the line between these different types of data continues to blur. When combined, two pieces of data previously considered non-personal could reveal attributes unique to an individual. Currently global regulatory policy, technology capabilities and commercial user interactions related to consent mechanisms are disconnected and piecemeal, solving individual industry or jurisdictional needs one at a time. As a result, policy and technology move at different speeds – while user experiences fall short. The creation of data exchanges for the common good presents a new opportunity to identify the interdependencies and draw the necessary connections between *policy* (i.e. internal governance), *technology* (i.e. data exchange reference architecture) and *commercial* (i.e. user experiences) as they relate to ensuring the consent and trust of individuals. These three pillars of the DCPI Consent and Trust Framework are defined in Table 1.

How is trust defined?

Trust can be enabled or eroded in many ways. The World Economic Forum describes digital trust as comprised of six primary elements: security, accountability, auditability, equity, ethics and transparency. While all are required elements of trust, the DCPI Consent and Trust Framework will not focus on security but will include trust attributes related to data protection and citizen understanding (see the section on *Building on the Digital Trust Framework to enable trust through consent mechanisms).*

FIGURE 1 **Six dimensions of digital trust**



Security (e.g. infrastructure confidentiality, integrity and availability, identity verification, hacking risks) is an important component of digital trust and will be covered in detail in the Data Marketplace Service Provider Rules and Governance Framework set to launch in 2022.

For guidance on baseline security measures, see the additional resources.

Additional resources

Advancing Cyber Resilience: Principles and Tools for Boards

3 The DCPI Consent and Trust Framework

The Framework is based on three interconnected pillars of trust: technology, policy and commercial interactions.

The Framework is structured around three pillars of trust for consent mechanisms: *technology*, *policy* and *commercial.*

TABLE 1 **Trust pillars**

DCPI Consent and Trust Framework		
Technology – data exchange reference architecture	**Policy – internal governance**	**Commercial – user interactions**
The technological capabilities, provided through data exchange operators, participants and individuals/users	The internal governance rules and processes created for consent mechanisms instituted and enforced by data exchange operators	The user interaction points and experiences related to permissioning mechanisms in a data exchange. Other areas of commercialization, such as data valuation, pricing mechanisms and further responsibilities of data exchange operators will be covered in other DCPI workstreams

Each of the three pillars of the DCPI Consent and Trust Framework is designed to be led (and managed) by different groups in an organization or different functional groups across stakeholder communities. In this framework, each pillar is described separately and focuses on areas of leadership among the attributes of the framework.

Although described as distinct areas of focus, the interconnections between the three pillars are both significant and critical for the overall success of a data exchange. Given the high levels of investment and rapid technology innovation in the emerging field of "big data", the cycle times for technology simply outpace the evolution of regulatory reform and change. Given that regulations have not yet been formally established in many areas, data exchange operators have the opportunity to collaborate with technology and commercial stakeholders to establish innovative, trustworthy, commercially sustainable and legally compliant approaches.

BOX 4 **Implementation note**

It is critical that **business processes** are implemented to support the consent mechanisms. This framework focuses on the attributes of building trust through consent mechanisms and does not provide details on business process implementation. The importance of the role of business processes in creating a successful data marketplace is undeniable; before launching, operators should ensure they have the internal structure in place to support consent mechanisms.

3.1 Technology – data exchange reference architecture

Although described as distinct areas of focus, the interconnections between the three pillars are both significant and critical for the overall success of a data exchange.

Creating trust through consent mechanisms requires user experience-related *technology* implementations that are intuitive. The major challenge in creating any framework is striking the balance between boundaries and innovation. To support both, the *technology* pillar focuses on the goals and effects rather than the actual definitions of technical solutions. These goals and effects focus on designing intuitive experiences for data exchange operators, participants and individuals, while enabling expected outcomes that are repeatable across data-sharing use cases and data exchanges. In addition, this pillar will evaluate technical solutions to support individual control of passively collected data. The *technology* pillar intends to uphold the following approaches to create trust when designing technical architecture to support data exchanges.

1. **User control supported by back-end systems:** support an agreed approach to an individual's control over any data about them that is collected, used and shared, both:
    a. In presentation to the individual
    b. On back-end interpretations of the defined purpose and limits of data use.
2. **Open APIs and standard libraries:** encourage minimal technology lock-ins. No proprietary solutions requiring licensing should be used. Open APIs, open-source licences and standard libraries are recommended.
3. **Privacy by default:** require technical data protection and privacy by design and default and enforce it by embedding trust controls, supported by privacy-enhancing techniques and other technologies (e.g. ad blockers) that reduce the risk of reidentification of the individuals to the level they require and which effectively protect against "singling out" of a data subject in a larger group.
4. **De-identification capabilities:** have the capability to generate strict separation between data and data owner through replacement of direct and indirect identifiers, and attribute information with values that are not relinkable to the identity of an individual. Recognize the limitations and balance the risk of reidentification.
5. **Technical controls:** enable technical controls to enforce analogue measures such as power of attorney, data collaboratives or data trusts.
6. **Access controls:** enforce access controls protecting unauthorized usage of the data exchange and data, including introducing mechanisms that allow verification of who used the data and when and how the data was used.
7. **Integrated data-management system:** establish and maintain an integrated data-management system to enable information review and analysis, taking into consideration the volume of data collected, requirements for analysis and interpretation of trends, speed of access and processing, among others. Data exchange operators should consider ease of data entry, strict control of data quality, automatic recognition and reporting of potential errors and accounting for various data formats (e.g. geographical coordinates, images, text, numeric).

3.2 Policy – internal governance

Policy related to consent mechanisms is intended to focus on **internal governance (in scope)**, including individual data exchange governance rules created and enforced by data exchange operators. **Regulatory policy (out of scope)** will not be addressed; the World Economic Forum and its DCPI Consent and Trust Framework does not make recommendations regarding regulatory policy.

There are multiple stakeholders in the ecosystem of data exchange. These include the individuals

who own the data, the data providers who collect, process and store the data on behalf of the data owners, and the data consumers, who participate in the exchange and access the data with appropriate consents and create innovative services of value to the individuals and organizations. Creating the appropriate internal governance structure for these stakeholders is a key enabler when building trust in the data exchange ecosystem.

The following principles guide the formulation of rules and mechanisms relating to the internal governance of data exchanges.

1. **Credible management:** the Governing Board is designed to evoke the confidence of the ecosystem stakeholders and individuals.
2. **Published policies:** the rules of business, privacy policy, security policy, the consent management framework and performance reports of the exchange are published for external audiences.
3. **Engagement rules:** the process for registering participants and the rules that govern their engagement are fair, equitable and transparent.
4. **Grievance handling:** mechanisms are robust, efficient, effective and transparent.
5. **Supervisory responsibilities:** the exchange ensures stakeholders: (1) comply with engagement rules and the applicable data protection regulations; and (2) have sound data governance mechanisms.

3.3 Commercial – user interaction

In the context of the DCPI Consent and Trust Framework for data exchanges, *commercial* applications of consent mechanisms refer to the direct individual/user interaction points – for example, when an individual is onboarded into the data exchange and consents to share data, or when additional data-sharing opportunities arise and are presented to the individual. As far as possible, *policy* should guide the design of these user interaction points and *technology* should be used as an enabler. Currently, they are primarily driven by *technology*, but the increasing complexity of the information presented and the need for education raise the importance of a focus on user interactions and user experiences. While the existing *technology* capabilities will drive the back-end implementation and may have limitations, the *commercial* needs will guide user-experience decisions at each user interaction point, unless specified by jurisdictional *policy*.

Opportunities for user interaction will happen under five primary scenarios:

1. **Education:** the user is being educated about the intended outcomes and operations of data exchange and different data-sharing processes where consent to contribute data can be granted
2. **Consent grant:** the user is performing the act of granting consent to use their data within the context of a particular use case
3. **Consent revocation:** the user is performing the act of revoking consent to use their data
4. **Resulting impact:** the consequences of granting consent to process data for different purposes, these interactions can come in many forms, including consent management/changes, consent renewals, disputes and recourse, and any other resulting individual impact
5. **Consent oversight:** the tools that enable the user to see and understand how the data produced by and about them is being used and the resulting outcomes of that use. Outcomes can be depicted both for an individual (e.g. what decisions are being made about them, what data informed that decision and what additional outcomes it will likely drive) as well as the greater societal good

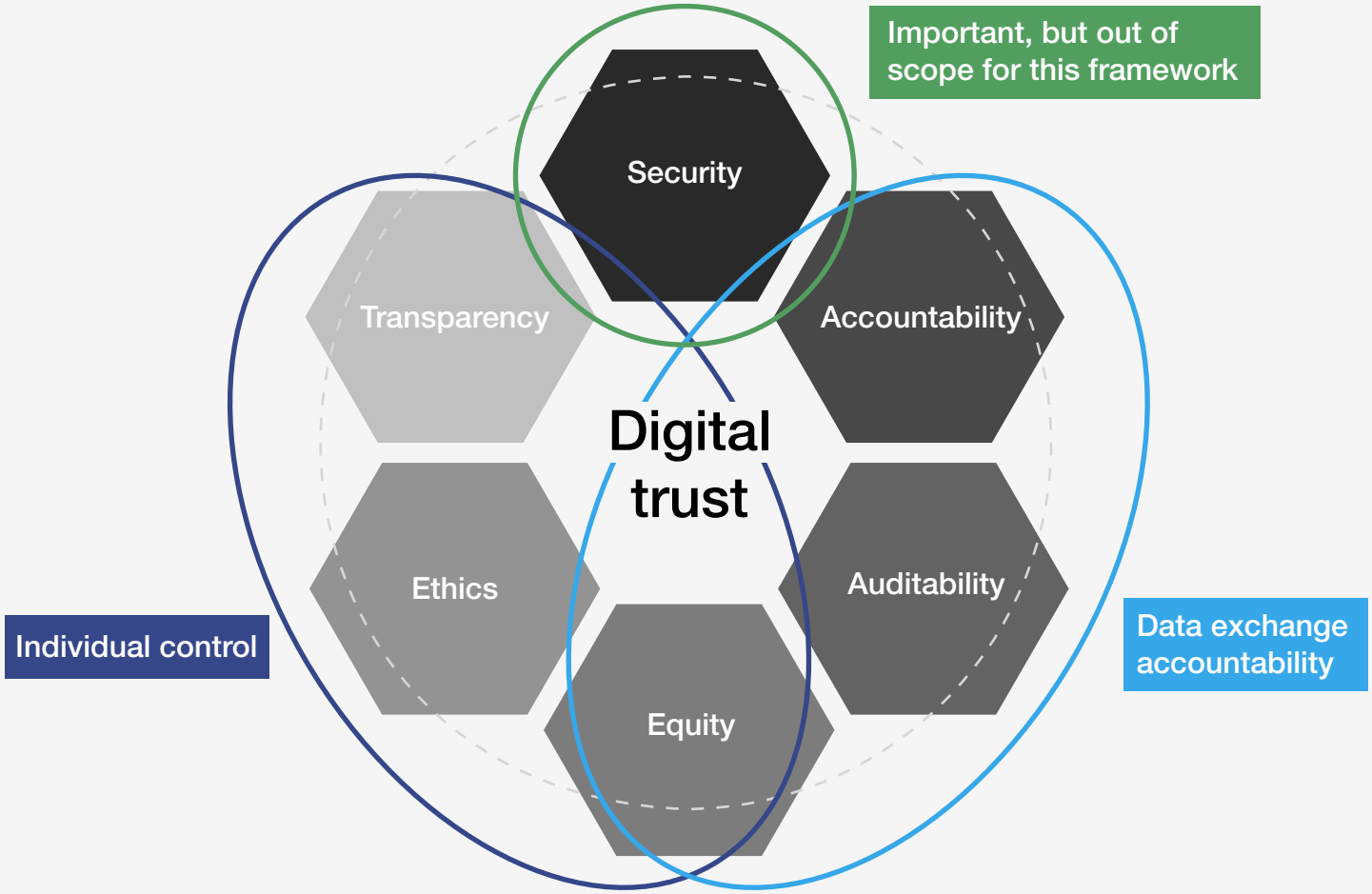
These individual interaction points provide opportunities for operators to build trust with the individuals who are contributing their data. Creating an environment in which individuals feel educated and supported to control how their data is used (in cases where it is appropriate) will be a critical success factor for the long-term success of data exchanges.

4 Expanding the Forum's Digital Trust Framework for consent and permissions

The Framework includes four groups of attributes that can help build trust in a data exchange.

The DCPI Consent and Trust Framework includes four groups of attributes that, when enabled through consent mechanisms, can help build trust in data exchanges: data exchange accountability, data protection, individual understanding and individual control. While individual control and data exchange accountability map directly to the Forum's Digital Trust Framework, building trust through consent mechanisms also requires consideration of data privacy and individual understanding attributes.

FIGURE 2 **Consent mechanism additions to the Forum's Consent and Trust Framework**



4.1 Trust attribute groups

The DCPI Consent and Trust Framework consists of four trust attribute groups, described in Table 2. Within each group, there are multiple attributes, each led by one or more pillars (*technology, policy, commercial*) and enabled through the other(s). The following section, Trust attributes for consent mechanisms, provides a high-level description for each attribute.[11]

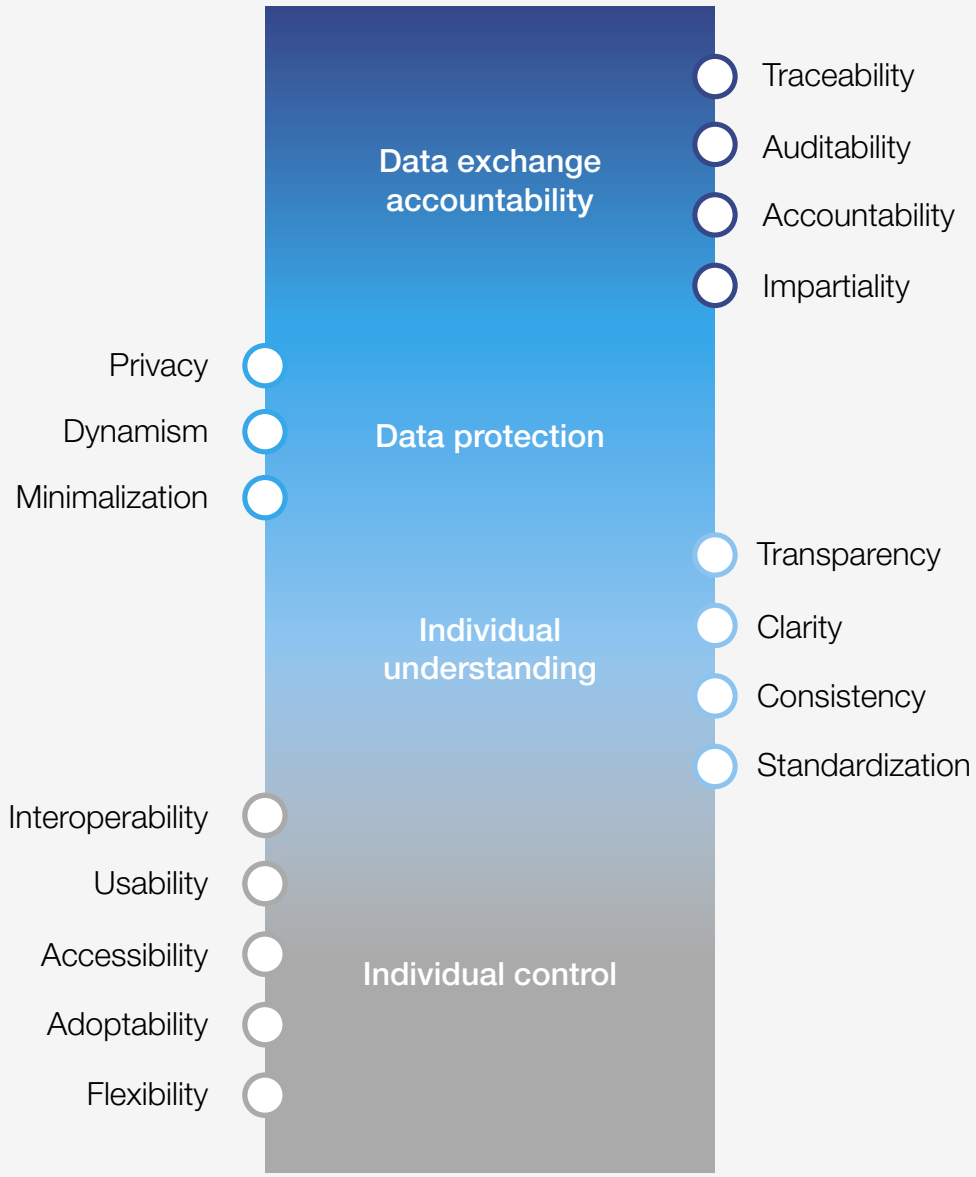
TABLE 2 **Trust attribute groups for consent mechanisms**

Pillars	DCPI Consent and Trust Framework		
	Technology – *data exchange reference architecture*	Policy – *internal governance*	Commercial – *user interactions*
Trust attribute groups	Data exchange accountability	Measuring, tracking and reporting how data moves through and outside of the data exchange	
	Data protection	Protecting data and reducing risk associated with the data that is stored within a data exchange (i.e. data at rest), data being processed (data in use) and data flows within, to and from (i.e. data in motion) a data exchange	
	Individual understanding	Educating individuals and positioning them to make informed choices on how data is collected, used and shared through a data exchange	
	Individual control	Supporting the tools and interfaces that enable individuals to exercise their informed choices on how their data is collected, used and shared through a data exchange	

4.2 Trust attributes for consent and permissions

The DCPI Consent and Trust Framework focuses on 16 attributes (Figure 3) for building trust through consent mechanisms in data exchanges for the common good. The concepts introduced in this framework are part of a much larger narrative that addresses the additional consent challenges associated with the very large amounts of data that are passively collected through internet of things (IoT) devices, analysed in inscrutable artificial intelligence (AI) systems and controlled by highly politicized decision-makers.

FIGURE 3 **Trust attributes for consent and permissions**



These attributes, when addressed through consent and permissioning in data exchanges, can dramatically improve trust in the system. While these are not the only needs to address when building trust, they are essential for consent mechanisms. There are also obvious connections between attributes that are not discussed here.[12]

4.2.1 Data exchange accountability

Measuring, tracking and reporting how data moves through and outside of the data exchange:

Traceability: the ability of data exchange stakeholders to follow their data from consent, through collection, use[13] and sharing, to termination – including the first and n^{th} generation of consumption levels. The current technical limitations need to be recognized and governance designed to accommodate future approaches

Auditability: data exchange operators and participants should maintain, for a period equal to the respective jurisdictional retention period for recourse of data misuse or other requirements a record of: (1) each instance of data collection, use or sharing; and (2) consent choices for data use explicitly provided by the individual to support audits

Accountability: any participant or data exchange operator is accountable for protecting individuals' privacy, providing methods for recourse, and using their data only within the consent parameters they or a third party who is legally acting on behalf of the individual (e.g. parent, guardian, data cooperative, trusted agent) have chosen. When at all possible, this extends to any additional processing of data outside of the exchange participants

Impartiality: all stakeholders who participate in a data exchange, regardless of entity size, stature or other potential biases, should be held equally accountable to the actions they take within a data exchange

4.2.2 Data protection

Protecting data and reducing risk associated with the data that is stored within a data exchange (i.e. data at rest), data being processed (data in use) and data flows within, to and from (i.e. data in motion) a data exchange:

Privacy: individuals should be provided with consent-management tools and experiences to control the collection, use and sharing of personally identifiable (PI) data and data of personal origin, in coordination with the rights afforded to individuals through data privacy policies within their jurisdictions. Data exchange operators are responsible for enforcing these user controls

Dynamism: data exchange operators provide participants with governance rules and enforce an individual's ability to grant, modify and revoke consent for data collection, use or sharing. In scenarios where consent modification and revocation are limited, such limits are communicated to users in advance of the initial permissioning experience

Minimization: individuals' data collection, use and sharing should be done in accordance with their consent choices, ensuring they are strictly relevant and adequate for a specific purpose. Data exchange participants enable the necessary tracing and audit capabilities for operators to ensure compliance

4.2.3 Individual understanding

Educating individuals and positioning them to make informed choices on how data is collected, used and shared through a data exchange:

Transparency: individuals can access clear information in due time and with ongoing visibility on how an entity collects, uses and shares their data, the potential risks and benefits of the service, the availability of source code, the rules and standards upon which it is based, their rights and obligations, and the governance structure of the data exchange

Clarity: individuals are enabled to have a clear understanding of how and why data is collected, used and shared. Consent choices are presented in a coherent and intelligible way. No dark-pattern behaviour is permitted

Consistency: consent mechanisms are presented to individuals in the same format across all user interactions in the data exchange (e.g. terminology, icons, structure)

Standardization: consent choices are presented to individuals, across use cases and participants, in a common, digestible format. Participants enable the necessary technology to read, interpret and implement consent choices received in the standard format. Operators enforce these standards

4.2.4 Individual control

Supporting the tools and interfaces for individuals to exercise their informed choices on how their data is collected, used and shared through a data exchange:

Interoperability: transfer capabilities for individuals' data, along with the associated rights and permissions, from one operator or participant to another operator or participant are in a common machine-readable format that is interpretable and understood across participants in a data exchange

Usability: individuals are able to control how their data is used, collected or shared. They are enabled, though the data exchange consent mechanisms, to act to control the collection, use and sharing of personally identifiable data as well as de-identified data of personal origin (in jurisdictions where required by law)

Accessibility: individuals are able to control how data is collected, used and shared through a simple consent-mechanism interface that is available at relevant interaction points. Access should be available for all individuals, including minorities, those with disabilities and individuals of low socioeconomic status

Adoptability: the governance approach for individuals' interactions with consent mechanisms should be implementable and manageable by both operators and participants in a data exchange

Flexibility: consent interfaces allow for easy modification to respond to the altered circumstances of operators, participants or individuals, as well as governance rules, regulatory policy or technology developments

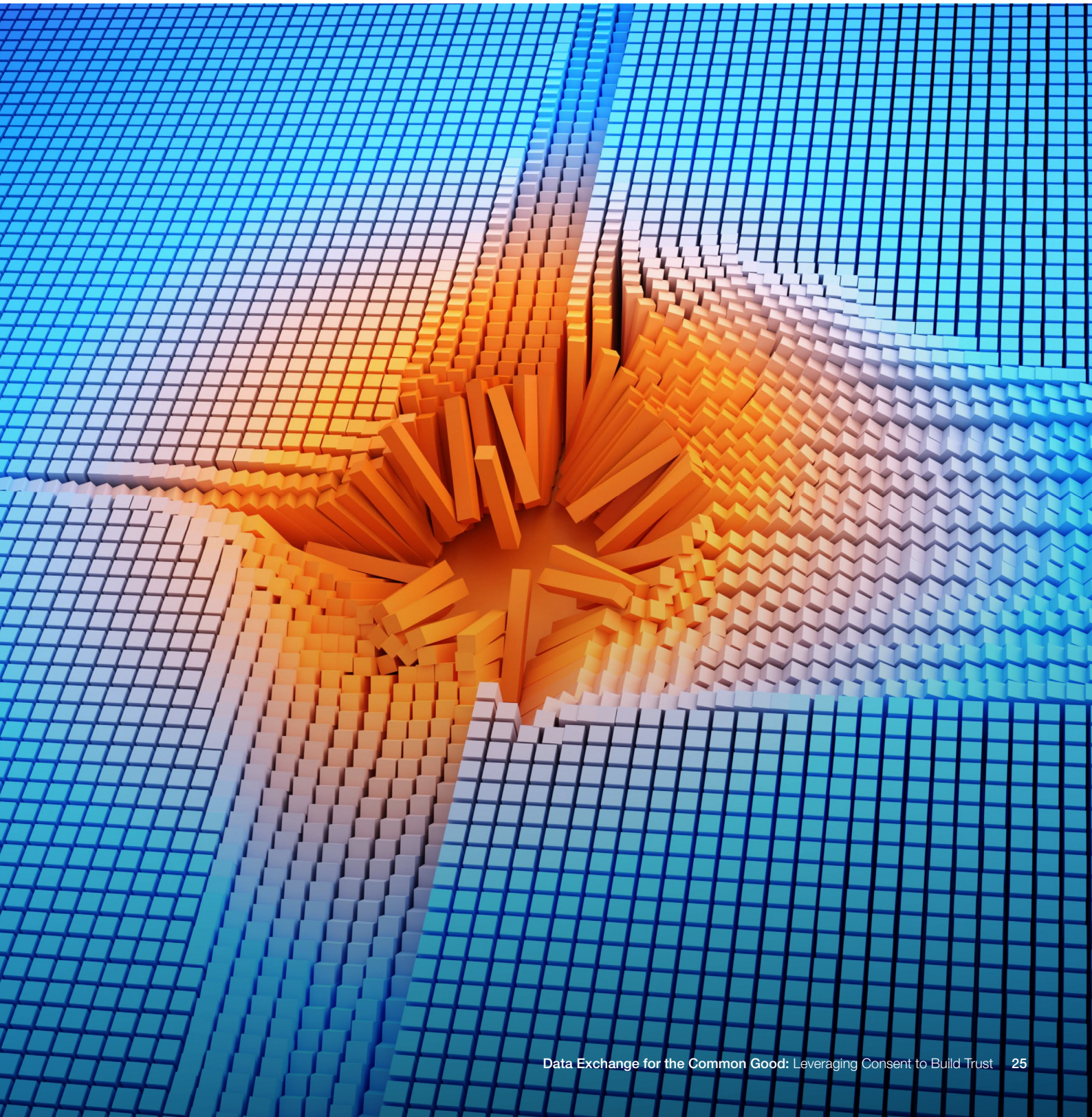
5 A future of individual trust in data exchanges

It is time to commit to a more informed, individual-empowering path forward.

Over the past few decades, the digital world has been a breeding ground for bad actors and dark patterns of data use. Shifting individuals' perceptions is no easy task, and a perfect solution does not yet exist. That said, there are still many opportunities, especially in systems that are still being designed, for data exchange operators and participants to recognize the errors of the past and choose a more informed path forward.

The key to building greater trust in data exchanges for the common good is a commitment from data exchange operators and participants around the world to test and pilot the DCPI Consent and Trust Framework. The first step is to examine the areas of data exchange accountability, data protection, individual understanding and individual control through three lenses in the overall system design: *technology* (data exchange reference architecture), *policy* (internal governance) and *commercial* (user interactions).

Some governments around the world have begun establishing functioning data exchanges and, while near-term data exchange cases may not require an individual's consent, they recognize the importance of establishing the right governance process immediately. The framework is the first DCPI release in a series of toolkits and pilot programme evaluations to test and improve implementation options and strategies for building trust through consent mechanisms in data exchanges.



Appendix: DCPI workstreams

DCPI workstreams and projects

Data marketplace service providers: Centre for the Fourth Industrial Revolution Japan

The World Economic Forum's Centre for the Fourth Industrial Revolution Japan (C4IR Japan) published the briefing paper *Developing a Responsible and Well-Designed Governance Structure for Data Marketplaces* under the global DCPI umbrella. This briefing paper extracts insights from discussions with thought leaders and experts to serve as a point of departure for governments and other members of the global community to explore governance structures for data marketplace service providers (DMSPs) – likely the primary operators and managers of data exchanges as trusted third parties, in data exchanges in a wide range of jurisdictions. The DCPI will further explore the concrete governance model predicated on fair, neutral and trusted DMSPs, which would be applicable to each jurisdiction and adaptable as per local contexts, through further discussion with the global community, followed by providing a toolkit for policy-makers.

Data valuation

The data valuation workstream focuses on developing a framework to effectively and fairly assess the value of data. By fairly assessing the value of data, a data exchange will create value for society and business. The initiative is currently developing a toolkit for data valuation and working closely with the Centre for the Fourth Industrial Revolution Affiliate Centre in Colombia's Moonshot project.

Centre for the Fourth Industrial Revolution Partners

Centre for the Fourth Industrial Revolution India

In collaboration with the DCPI community, the Centre for the Fourth Industrial Revolution India shared its vision of a data exchange through a white paper *(Towards a Data Economy: An Enabling Framework).* In this paper, the following frameworks for a data exchange were detailed:

- A reference model that lays down the functional capabilities of a data exchange
- A 3P (protect-prevent-promote) approach to governance of a data exchange ecosystem
- A need to incentivize data sharing among public- and private-sector stakeholders
- Enablers for a data exchange ecosystem to flourish

With a view to turning this concept into reality, the Centre for the Fourth Industrial Revolution India, in collaboration with the Telangana state government, the Telangana State Agriculture University and other stakeholders, is working to pilot an agriculture data exchange.

Centre for the Fourth Industrial Revolution Colombia

The Colombian government, with the support of the Centre for the Fourth Industrial Revolution Colombia, is leading the creation of a regulatory framework for data exchange through the National Data Infrastructure Plan, which contains a roadmap to transition to data-driven economies. A multistakeholder group has addressed the main challenges when implementing and managing data exchanges for the common good. Key goals include:

- Increasing the reuse of the data that makes up the data infrastructure
- Consolidating a data-driven public sector
- Promoting innovation
- Promoting the development and integration of emerging technologies and AI
- Establishing agile data governance models for a data-driven digital economy
- Positioning Colombia as a benchmark in the use of data for the digital economy
- Building an environment of public trust for the use of and protection of data

Contributors

Lead Authors

Kimberly Bella
Senior Director, Global Strategic Initiatives, Visa; World Economic Forum Fellow, United States

Christophe Carugati
Senior Policy Analyst, Center for Data Innovation, Belgium

Cathy Mulligan
Professor and DCentral Lab Director, Instituto Superior Technico, Portugal

Marta Piekarska-Geater
Founder, Private Fox, United Kingdom

Acknowledgements

Brinson Elliott
Analyst, The Cantellus Group, United States

Katelyn Hamrick
Senior Analyst, Visa, United States

Zohar Hod
Founder and Chief Executive Officer, One Creation, United States

Katherine Hsiao
Senior Executive Advisor, Palantir Technologies, United States

Henrik Hvid Jensen
Chief Technology Officer, DXC Technology, Denmark

Kibae Kim
Fellow, World Economic Forum, South Korea

Gary LaFever
Chief Executive Officer and General Council, Anonos, United States

Grace Lykins
Director, Visa, United States

Ran Melamed
Head of Business Development, Orbs, Singapore

Akhila Satish
President, Meseekna, United States

Karen Silverman
Chief Executive Officer and Founder, The Cantellus Group, United States

Sofie Stenbog
Product Owner, Data for Good Foundation

Endnotes

1. Kudo, Fumiko, quoted in World Economic Forum, *Good Data*: *Sharing Data and Fostering Public Trust and Willingness*, April 2021: https://www3.weforum.org/docs/WEF_Good_Data_Sharing_Data_and_Fostering_2021.pdf.
2. Morris, Chris, "The Number of Data Breaches in 2021 Has Already Surpassed Last Year's Total", *Fortune*, 6 October 2021: https://fortune.com/2021/10/06/data-breach-2021-2020-total-hacks/.
3. Confessore, Nicholas, "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far", *The New York Times*, 4 April 2018: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.
4. Lecher, Colin, "FTC Officially Rules that Cambridge Analytica Deceived Facebook Users", *The Verge,* 6 December 2019: https://www.theverge.com/2019/12/6/20999078/ftc-cambridge-analytica-facebook-users-official-ruling-privacy-scandal.
5. Civil Code – CIV; Division 3. Obligations [1427–3273.16] (Heading of Division 3 amended by Stats. 1988, Ch. 160, Sec. 14.); Part 4. Obligations Arising from Particular Transactions [1738–3273.16] (Part 4 enacted 1872.); TITLE 1.81.5. California Consumer Privacy Act of 2018 [1798.100–1798.199.100] (Title 1.81.5 added by Stats. 2018, Ch. 55, Sec. 3.) 1798.140. Definitions: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.140.&highlight=true&lawCode=CIV&keyword=dark+patterns.
6. Patel, Sanjay, "'Dark Patterns' and Data Protection Compliance", *Trilateral Research*, 1 October 2021: https://www.trilateralresearch.com/dark-patterns-and-data-protection-compliance/.
7. Question: In general, how concerned are you about the privacy of your information when conducting digital activities (e.g. send/receive email/text/instant messages, stream videos/TV/movies, listen to music, access social networks, read news/magazines/blogs, conduct research, buy physical or digital items, sell products/services, use location services, manage finances) either online or on a mobile device? Source: Visa/Kearney Data Privacy Study (US N=5,215, UK N=5,252, AUS N=800, SG N=1,000, HK N=1,000, JP N=2,500).
8. Q30: In most cases, who benefits more when you allow your consumer data to be collected and used by a company? Source: 2020–2021 Visa Consumer Empowerment Study (US, UK, Australia, N=6,000).
9. Laidler, John, "High Tech is Watching You", *The Harvard Gazette*, 4 March 2019: https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/.
10. Q29: Which of these approaches comes closes to your opinion when it comes to controlling the use of your consumer data? Source: 2020–2021 Visa Consumer Empowerment Study (US, UK, Australia, N=6,000).
11. In the next publication, the DCPI Consent and Trust Toolkit will outline the key questions and implementation options for each attribute.
12. While there are also many connections and dependencies between different attributes across attribute groups, they have been omitted from this paper and will be described in detail in the accompanying DCPI Consent and Trust Toolkit, set to be released in 2022.
13. Recognizing the difficulties associated with tracing data outside of a closed system, in inscrutable AI black boxes and in other scenarios, the framework seeks to highlight the importance of traceability in building trust.

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