February 2020 · Aline Blankertz

Designing Data Trusts

Why We Need to Test Consumer Data Trusts Now

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Executive Summary

Daten über Personen, ihre Vorlieben und ihr Verhalten werden für Unternehmen, Behörden und Forschungseinrichtungen zu einer immer wichtigeren Ressource. Verbraucher:innen müssen entscheiden, welche der Daten über sie zu welchem Zweck weitergegeben werden. Dabei möchten sie einerseits sicherstellen, dass diese nicht dazu verwendet werden, vertrauliche Einzelheiten ihres Privatlebens zu erschließen oder andere unerwünschte Zwecke zu verfolgen. Andererseits profitieren sie gern von personalisierten Produkten und Innovationen, die mithilfe derselben Daten entstehen. Die Datenerfassung ist so komplex, dass Verbraucher:innen überfordert sind und viele von ihnen Datenschutzerklärungen resigniert akzeptieren, ohne zu wissen, welche Konsequenzen daraus entstehen. Sie verlieren das Vertrauen, dass diejenigen, die so die effektive Kontrolle über die Daten erlangen, sie auch zum Nutzen der Verbraucher:innen verwenden.

Gleichzeitig sammeln und speichern einige wenige große Unternehmen riesige Datenmengen, die es ihnen ermöglichen, Erkenntnisse über Märkte und Verbraucher:innen hinweg zu nutzen. In Europa hat die Datenschutzgrundverordnung (DSGVO) den Verbraucher:innen Rechte eingeräumt, um ihre Interessen gegenüber diesen Unternehmen durchzusetzen. Doch auch mit der DSGVO haben Verbraucher:innen weder genug Informationen noch genug Macht, um sich Gehör zu verschaffen. Andere Organisationen, vor allem kleine Unternehmen oder Start-ups, haben keinen Zugriff auf die Daten (es sei denn, einzelne Nutzer:innen nutzen mühsam ihr Recht auf Portabilität), was oft Wettbewerb und Innovation im Wege steht.

Viele europäische Regierungen arbeiten an Konzepten, um produktive Datennutzung mit dem Schutz der Privatsphäre in Einklang zu bringen. In den letzten Monaten haben sich Datentreuhänder als eine vielversprechende Möglichkeit herauskristallisiert, um einen an den Interessen der Verbraucher:innen orientierten Datenaustausch zu ermöglichen. Das Konzept wird von so unterschiedlichen Gruppen wie Datenschützer:innen, Unternehmen und Expert:innenkommissionen gleichermaßen unterstützt. In Deutschland beispielsweise haben die Datenethikkommission und die Kommission Wettbewerbsrecht 4.0 empfohlen, Datentreuhänder weiter zu untersuchen. Auch die Bundesregierung ist dabei, das Konzept in ihre Datenstrategie aufzunehmen.

Es gibt bisher kein allgemeines Verständnis davon, was Treuhänder für Verbraucher:innendaten sind und was sie tun. Um die erwähnten Probleme zu

adressieren, ist es sinnvoll, Datentreuhänder wie folgt zu verstehen: Sie sind Vermittler, die die Interessen von Verbraucher:innen aggregieren und sie gegenüber datennutzenden Organisationen vertreten. Datentreuhänder haben tiefere technische und juristische Expertise sowie mehr Verhandlungsmacht, um mit Organisationen über die Bedingungen der Datennutzung zu verhandeln. So können sie bessere Ergebnisse erzielen, als Verbraucher:innen das einzeln könnten. Um ihren verbraucher:innenorientierten Auftrag zu erfüllen, sollten Datentreuhänder in der Lage sein, Zugriffsrechte zuzuweisen und sicherzustellen, dass das umgesetzt wird, was zwischen Verbraucher:innen und Unternehmen ausgehandelt wurde. Sie können, müssen aber nicht selbst Daten speichern.

Die breite Zustimmung zur Idee des Datentreuhänders könnte auch damit verbunden sein, dass es nur wenige praktische Beispiele oder Ideen für die Umsetzung gibt. Ob die hohen Erwartungen, die an sie gestellt werden, erfüllt werden können, hängt entscheidend damit zusammen, wie Datentreuhänder konkret umgesetzt werden. Politische Entscheidungsträger:innen sollten sich deshalb mit der komplexen Ausgestaltung von Datentreuhändern befassen, indem sie zunächst die unmittelbar bevorstehenden Herausforderungen für die Umsetzung lösen:

Erstens: Wie können wir sicherstellen, dass die Interessen des Treuhänders mit denen der Verbraucher:innen, die er vertritt, in Einklang stehen? Die rechtliche und finanzielle Struktur muss Verbraucher:innen klar erkennen lassen, dass der Datentreuhänder in ihrem Interesse handelt. Zu diesem Zweck könnten eine Anschubfinanzierung aus öffentlichen Quellen, eine Datensteuer oder -abgabe oder ein Mitgliedsbeitrag die Kosten eines Datentreuhänders tragen.

Zweitens, wie können wir es den Verbraucher:innen leicht machen, ihre Interessen auszudrücken? Damit Verbraucher:innen einen Datentreuhänder nutzen können, muss er die Komplexität der "informierten Einwilligung" reduzieren können und stattdessen seine Arbeit auf Entscheidungen basieren, die Verbraucher:innen zu treffen in der Lage und bereit sind. Damit ein Datentreuhänder ihre Interessen vertreten kann, müssen Verbraucher:innen ihre Datenrechte delegieren können, möglicherweise stärker, als die DSGVO es vorsieht. Das könnte zum Beispiel erreicht werden, indem die Möglichkeit der Repräsentation (Artikel 80) auf die Ausübung von Datenrechten ausgeweitet wird oder indem Verbraucher:innen ermöglicht wird, ihr Recht auf Erteilung (und Widerruf) einer Einwilligung zu delegieren, wozu Datentreuhänder einen besonderen rechtlichen Status erhalten könnten.

Drittens, wie können Organisationen motiviert werden, mit Datentreuhändern zu arbeiten? Datentreuhänder sollten so gestaltet sein, dass sie es Organisationen einfach machen, Daten im Einklang mit den Interessen von Verbraucher:innen zu nutzen. Die Aussicht auf Zugang zu mehr Daten und mehr Rechtssicherheit kann für viele Organisationen, insbesondere für kleine Unternehmen, ausreichen, um mit einem Datentreuhänder zu verhandeln.

Praktische Tests und Pilotprojekte sind jetzt notwendig. Nur so kann ermittelt werden, ob Datentreuhänder tatsächlich Verbraucher:innen ermächtigen können, ihre Interessen besser durchzusetzen, als sie es aktuell können. Auch die Frage danach, wie genau sie zu diesem Zweck zu gestalten sind, kann nur in der Interaktion mit Nutzer:innen beantwortet werden. Erst dann ergibt es Sinn, weitere Schritte wie Richtlinien, Regelungen oder andere Formen der Gesetzgebung in Betracht zu ziehen, um z.B. sicherzustellen, dass auch schutzbedürftige Verbraucher:innen von Datentreuhändern profitieren und Unternehmen sie nicht umgehen können. Datentreuhänder kritisch zu testen kann sich im derzeitigen Rechtsrahmen als schwierig erweisen, da er das dafür nötige Maß an Delegierung von Einwilligungs- und Datenrechten an eine vertrauenswürdige Instanz nicht zulässt. „Regulatorische Sandkästen“ (regulatory sandboxes) könnten die geeigneten Schutzvorkehrungen für die Prüfung von Datentreuhänder bieten – mit strenger Aufsicht und hohen Transparenzanforderungen. Das würde uns ermöglichen, dass mehr Daten zum Nutzen von Verbraucher:innen fließen.

Contents

1. Introduction

Data is at the heart of two European debates: It is said that consumers should have control over what happens with data about them. However, companies are under pressure to adopt more data-driven business models, and share and collaboratively use their data to ensure global competitiveness. The General Data Protection Regulation (GDPR) provides a framework for privacy but consumers are overburdened with the requirement of "informed consent." A few powerful companies effectively control how data is used by whom.

Data trusts have emerged as a potential solution to enable data-sharing for consumers' benefit. Expert groups have endorsed the concept: The review in "Growing the artificial intelligence industry in the UK" recommended developing data trusts to "ensure [data] exchanges are secure and mutually beneficial."[1] German commissions on data ethics (Datenethikkommission) and on competition law 4.0 (Kommission Wettbewerbsrecht 4.0) suggested that data trusts could help individuals take control over data about them and foster competition in data-driven markets.[2] The idea of using automation to help consumers overcome the burden of information related to privacy and data-sharing goes back to at least 2013, when the World Economic Forum introduced trustworthy "recommender systems."[3]

However, few data trusts or similar organizations representing consumers' interests in the data economy exist in practice. Although experts appear to agree that the concept is appealing, they find it difficult to agree on how data trusts can and should be implemented.

---

1 Hall, Dame Wendy and Jérôme Pesenti, 'Growing the Artificial Intelligence Industry in the UK', Department for Digital, Culture, Media & Sport and Department for Business, Energy & Industrial Strategy, 15 October 2017, Recommendations of the Review, https://www.gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk/recommendations-of-the-review.

2 See Kommission Wettbewerbsrecht 4.0, 'Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft: Bericht der Kommission Wettbewerbsrecht 4.0', German Federal Ministry for Economic Affairs and Energy, September 2019, section V.3.c, https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/bericht-der-kommission-wettbewerbsrecht-4-0.pdf?__blob=publicationFile&v=10;
Datenethikkommission der Bundesregierung, 'Gutachten der Datenethikkommission', Potsdam, Bundesministerium des Innern, für Bau und Heimat, 2019, section 4.3, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=5.

3 World Economic Forum, 'Rethinking Personal Data: Trust and Context in User-Centred Data Ecosystems', Geneva, Switzerland: World Economic Forum, May 2014, http://www3.weforum.org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014.pdf.

This paper describes the minimum requirements for a data trust as an alternative approach to data governance that is intended to enable data-sharing in consumers' favor. If data trusts are to find their way into practice, the minimum requirements provide a starting point for pilot projects to explore the usefulness of the concept in real-life circumstances. In the following, section 2 sets out the two key problems in the data economy: that consumers' interests hardly matter and that much of the value in data remains locked up by only a few companies. Section 3 explains how data trusts should be defined and designed to address these challenges. Section 4 describes the three imminent challenges for implementation and discusses preliminary solutions for resolving these problems. Section 5 concludes with a few reflections on how the concept could find its way into practice.

The data generated from smart home devices illustrates the concerns, and how data trusts could address those concerns. This industry is growing rapidly, with the potential to transform many aspects of private lives, but it relies on huge amounts of sensitive data. Finding a way to ensure that companies' data use benefits consumers could resolve concerns about invasion of privacy and boost trustworthiness and growth.

2. Challenges in the data economy

Data trusts can address two main challenges: First, consumers cannot assert their interests in the use of data that concerns them. Second, many organizations struggle to get access to data effectively controlled by a few large players.

2A. Consumers cannot assert their interests in the use of data about them

Consumers care about how data about them is used, but they have lost trust in companies to manage data about them in ways the consumers approve of. For example, many people appreciate the idea of having data rights but have limited ability to understand how and by whom data about them is being used.[4] Companies effectively control data about consumers and are free to do so if they comply with, in Europe, the GDPR. Companies get to offer to consumers how the organizations want to use data, allowing consumers to give consent (or decline). At the same time, it is cumbersome (using portability rights) if not impossible for consumers to share data about themselves with other organizations. For example, regarding smart homes, German consumers ranked online companies last when asked with whom they would be willing to share their smart home data, while two-thirds of those age 18–44 wanted to combine products from different providers.[5]

Leaving individuals to manage data about them, for example, by asking them to give informed consent under the GDPR, leads to market failure for various reasons:

- **excessive information cost:** As almost all types of devices and activities generate data that has a personal dimension, consumers cannot reasonably be expected to engage with the terms that govern the use of that data. A recent survey indicated that only a small fraction of Google users access the privacy policies, and 85% of those who do spend less than ten

4 See Samson, Renate, Kayshani Gibbon, and Anna Scott, 'About Data about Us', Open Data Institute, the RSA (Royal Society for the Encouragement of Arts, Manufacturers and Commerce), and Luminate, September 2019, https://www.thersa.org/globalassets/pdfs/reports/data-about-us-final-report.pdf.

5 Deloitte, 'Smart Home Consumer Survey 2018: Ausgewählte Ergebnisse für den deutschen Markt', Deloitte, May 2018, figures 17 and 19, https://www2.deloitte.com/content/dam/Deloitte/de/Documents/technology-media-telecommunications/Deloitte_TMT_Smart_Home_Studie_18.pdf.

seconds on the website.[6] German-language privacy terms for four voice assistants have been found to require 15 minutes of reading time, on average.[7] In addition, consumers should be able to assess and compare those notices and understand what risks and benefits the notices imply given current and future technological developments. For example, data collected today could be used to increase prices for some consumers in the future or to personalize products for assisted living in a smart home.

- **lack of bargaining power:** Consumers cannot credibly negotiate with organizations, because the latter have little incentive to respond to individual concerns or demand. Data-using organizations tend to generate value from large datasets, so the potential loss of individual customers is unlikely to affect the companies. Thus, consumers generally receive take-it-or-leave-it offers from organizations.[8]

- **context-dependent decisions:** Even when given a choice, consumers struggle to make consistent decisions about their privacy. For example, consumers reveal less about themselves when they are reminded of privacy concerns.[9] The amount consumers would be willing to spend to hold on to their data is also significantly higher than the amount they would be willing to spend on buying their data back if they believe their transaction partner already has it.[10]

- **collective dimension of data:** Data about one person allows for inferences about other people, creating a collective dimension where decisions about data-sharing affect not only the individual(s) involved in the data

6 Competition and Markets Authority, 'Online Platforms and Digital Advertising Market Study, Interim Report', December 2019.

7 Kettner, Sara Elisa, Christian Thorun, and Jan-Peter Kleinhans, 'Big Data im Bereich Heim und Freizeit Smart Living: Status Quo und Entwicklungstendenzen', ABIDA - Assessing Big Data, German Federal Ministry of Education and Research, 2018, https://www.abida.de/sites/default/files/Gutachten_HeimUndFreizeit.pdf.

8 Zuiderveen Borgesius, Frederik, Sanne Kruikemeier, Sophie Boerman, and Natali Helberger, 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation', European Data Protection Law Review, 3(3), 15 March 2018, pp. 353-368.

9 John, Leslie K., Alessandro Acquisti, and George Loewenstein, 'Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information', Journal of Consumer Research, 37(5), 2010, pp. 858-873.

10 Acquisti, Alessandro, Leslie K. John, and George Loewenstein, 'What Is Privacy Worth?,' The Journal of Legal Studies, 42(2), June 2013, pp. 249-274.

generation.[11] Correlation in datasets means that, for example, data about the everyday routine of young families as captured by their smart home devices is likely to provide information about a young family who may not wish to share their data. Thus, data shared by one group of people is likely to undermine, at least to some extent, efforts by other people who wish to protect their privacy.

As a result, consumers fail to assert their interests in how data about them is used. Instead, data flows follow the commercial interests of often dominant companies with little regard for the wider impact on society.

Some hope that stricter enforcement of the GDPR can address some of these concerns by ensuring, for example, that consent is given actively by opting in, and that consumers are sufficiently informed based on privacy notices that are presented in an appropriate situation.[12] Most of these efforts are directed at implementing what is often called "informational self-determination," a concept that has shaped the German and European notion of data protection. This concept aims to empower individuals to make informed choices about data about them, with limited interference by external parties. Different initiatives aim to give consumers more tools to exercise their rights and take a larger share of the value created by data markets.

11 Mantelero, A., 'Personal Data For Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection', Computer Law & Security Review, 32(2), 2016, pp. 238-255; Bergemann, Dirk, Alessandro Bonatti, and Tan Gan, 'The Economics of Social Data', Cowles Foundation Discussion Paper No. 2203, 25 September 2019; Choi, J. P., D. S. Jeon, and B. C. Kim, 'Privacy and Personal Data Collection With Information Externalities', Journal of Public Economics, 173, 2019, pp. 113-124.

12 Jentzsch, Nicola, 'Die persönliche Datenökonomie: Plattformen, Datentresore und persönliche Clouds', Deutsches Institut für Wirtschaftsforschung, 31 January 2017, https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_Gutachten_Die_persoenliche_Datenoekonomie_Anhang_2_final.pdf.

Current approaches for improving consumer control and share data more widely
Various approaches aim to give consumers more control over data flows and to automate consent for different types of data.

Personal information management systems (PIMSs), such as Digi.me, assist consumers in managing data about them; in contrast to data trusts, individual consumers remain responsible for making decisions about data. PIMSs help consumers solicit their data from data-collecting companies and can allow consumers to provide access to that data to other organizations. Bitsaboutme, a PIMS based in Switzerland, reports testing recommender systems to help their users assess offers more easily.

Privacy bots could help consumers communicate their privacy preferences to service providers, reducing the need to engage with individual services, and their data policies and settings. However, efforts by European organizations have often remained at the early stages.

Data marketplaces can help consumers monetize their data. For example, Streamr, a data marketplace based in the United Kingdom, gives its users the option to collect and sell their browsing data through a plug-in called Swash.

The **MyData movement** aims to "empower individuals by improving their right to self-determination regarding their personal data" and brings together organizations and individuals who share this objective.

In **health**, **biobanks** enable scientific research on anonymized data from different sources. For example, services such as those of ambulanzpartner.de provide patients with the opportunity to facilitate data exchange between their medical advisers and to donate data for research.

Although these approaches may alleviate some of the pain for consumers, the approaches do not fix the underlying failures of data markets because consumers are left with the burden of personal data management. A consumer data trust is a more comprehensive approach to shaping data markets for the benefit of consumers.

2B. Many organizations struggle to get access to data effectively controlled by a few large players

As data becomes an increasingly important resource for companies, such as for personalizing or offering data-driven complementary services, many organizations struggle to get enough data. For example, in the smart home, Amazon and Google have quickly expanded their product range, allowing them to use data from one market to improve their products in related markets. In addition, Amazon's and Google's broad product range increases the incentives for other providers to ensure compatibility with these market leaders. This is likely to lead to vast amounts of data being held by a small number of companies. Small companies and entrants generally cannot access that data to develop new services, even when it is in consumers' interests (unless consumers actively port their data using portability rights under Article 20). The GDPR may even aggravate this inclination to concentration, as the legislation tends to favor organizations with existing consumer relationships[13] that can more easily ask consumers to accept updated terms, rather than asking for consent to the terms of a new product, as rival providers have to do.

The limited availability of data can result in a tangible disadvantage in product development. Consumers tend to put usability ahead of other product features, including data policies. For example, Amazon contracted workers to transcribe voice recordings from its smart speaker Alexa without users' knowledge.[14] According to Amazon, this practice allows the company to improve its services.[15] Public outrage over the practice has not stopped Amazon from capturing a large part of the market. Small companies that, for example, adopt a strict opt-in policy for voice transcription are likely to struggle

13 Campbell, James David, Avi Goldfarb, and Catherine E. Tucker, 'Privacy Regulation and Market Structure', Journal of Economics & Management Strategy, 24(1), 2015, pp. 47-73. Evidence following enactment of the GDPR indicates that a reduction in third-party trackers for advertising has had limited impact on Google, Facebook and Amazon; see Libert, Timothy, Lucas Graves, and Rasmus Kleis Nielsen, 'Changes in Third-Party Content on European News Websites after GDPR', August 2018, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2018-08/Changes%20in%20Third-Party%20Content%20on%20European%20News%20Websites%20after%20GDPR_0_0.pdf.

14 Day, Matt, Giles Turner and Natalia Drozdiak, 'Amazon Workers Are Listening to What You Tell Alexa', Bloomberg, 11 April 2019, https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio.

15 Specifically, Amazon states in its Alexa Device FAQs that the training of Alexa voice recognition "relies in part on supervised machine learning, an industry-standard practice where humans review an extremely small sample of requests to help Alexa understand the correct interpretation of a request". See Amazon, 'Alexa and Alexa Device FAQs', https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230.

to offer voice recognition of comparable quality.[16] However, there is evidence that consumers do not oppose sharing voice data in principle, and may be willing to share their voice data if the conditions of use are transparent. Many consumers have contributed to the project "Common Voices" without compensation, helping to build an open-source dataset of human speech.[17] Doing so currently requires consumers to actively record speech, rather than being able to share voice samples that have been collected. A data trust could help organizations explore new forms of data-sharing in the interest of consumers, thus enabling wider use of data, as well as more innovation and competition.

16 Deutsche Telekom reportedly switched from opt-in to opt-out voice recording for their smart speaker due to difficulties in obtaining opt-in consent to train their models. See Scheuer, Stefan, and Dietmar Neuerer, 'Der Sprachassistent der Telekom soll Amazon herausfordern – Experten bemängeln Datenschutz', Handelsblatt, 22 October 2019, https://www.handelsblatt.com/technik/it-internet/hallo-magenta-der-sprachassistent-der-telekom-soll-amazon-herausfordern-experten-bemaengeln-datenschutz/25141186.html.

17 Common Voice, Mozilla Initiative, https://voice.mozilla.org.

3. Data trust definition and design

Data trusts can be one way of addressing the challenges of the data economy. To understand how, it is necessary to understand what data trusts are and how they should be designed to be effective. This section provides a tentative definition of data trusts by clarifying their position on a spectrum of data governance approaches and by describing what data trusts should do. The section also provides an overview of questions and options relevant to the design of consumer data trusts.

3A. A consumer data trust could help enable more data-sharing in the interest of consumers

Although data trusts have been widely endorsed, no clear definition has emerged. The lack of a clear definition is one of the challenges to implementing data trusts. However, it is also an opportunity, because the concept can evolve alongside evidence of how the data trust should be designed from legal, technical and governance perspectives. The notion used in the following is consistent with many of the current contributions to the debate.[18]

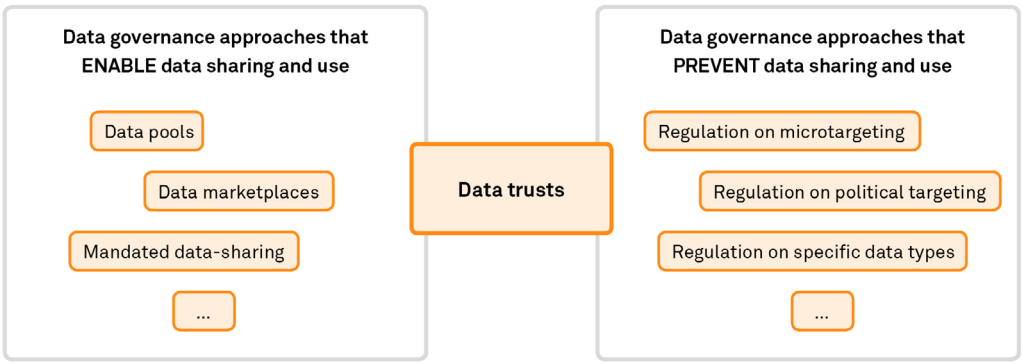
We envision data trusts for consumers as an intermediary that aggregates consumers' interests and represents them more effectively vis-à-vis data users. Data trusts would negotiate with organizations on the conditions of data use to achieve outcomes using more technical and legal expertise, as well as greater bargaining power than individual consumers can reasonably be expected to have.

Data trusts are different from many other approaches for facilitating or regulating data flows; see Figure 1. Data trusts restrict data uses that are not in consumers' interests, but also enable new data flows that are currently held back by data-hoarding companies. Approaches such as data pools or marketplaces are usually designed to facilitate more data exchange, as is proposed regulation to mandate data-sharing by large companies under

18 For example, Hardinges, Jack, Peter Wells, Alex Blandford, Jeni Tennison, and Anna Scott, 'Data Trusts: Lessons From Three Pilots', Open Data Institute, April 2019, https://docs.google.com/document/d/118RqyUAWP3WIyyCO4iLUT3oOobnYJGibEhspr2v87jg/edit and related work, Delacroix, Sylvie, and Neil D. Lawrence, 'Bottom-up Data Trusts: Disturbing the "One Size Fits All" Approach to Data Governance', International Data Privacy Law, ipz014, 2019; Ruhaak, Anouk, 'Data Trusts: Why, What and How', Medium, 12 November 2019, https://medium.com/@anoukruhaak/data-trusts-why-what-and-how-a8b53b53d34.

specific circumstances.[19] These approaches tend to be problematic in the context of personal data, as the GDPR requires consent or anonymization for wider data-sharing to be permitted. In contrast, approaches for preventing personal data from being shared and used generally address specific concerns about the use of data, for example, to target political content or sensitive information.

Figure 1 – Data governance approaches



Consumer data trusts sit in the middle in the sense that they are intended to prevent data-sharing and use that are to the detriment of consumers. Such practices exist where the interests of the organization that effectively controls the data conflict with those of consumers. Such a conflict may arise if, for example, a smart assistant knows about the consumer's search habits and consumption preferences, and proposes products that result in a higher margin for the manufacturer of the smart assistant (it does not matter if the manufacturer does so directly or if it sells the data to enable others to do so). However, data-controlling organizations may also suppress data flows that are not in their own interest but are beneficial for consumers. This type of situation can occur if consumers want to use the firms' previous data across services, but have no easy way of transferring it, or if they want to make their data accessible for products or services consumers support, such as research. Thus, data trusts are likely to make data more accessible to some and stimulate innovation and competition. Overall, data trusts reduce the influence of the companies that currently exert control over data about individuals and give more influence to consumers.

19 For example, the proposed reform of the German competition law considers the refusal to supply data that is essential for competition in upstream or downstream markets an abuse of dominance; see Bundesministerium für Wirtschaft und Energie (2020), ‚Entwurf eines Zehnten Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0'.

Consumer data trusts are just one type of data trust. Other types could be used to share machine data while ensuring that the shared data is compliant with competition law. Similarly, data trusts could be used to aggregate and share sensitive government data with other government agencies and/or citizens to address concerns about excessive data centralization. Although some challenges for these data trusts are likely to be identical to those for consumer data trusts, exploring the design of non-consumer data trusts is beyond the scope of this paper.

3B. A data trust must provide access and support enforcement

Defining the tasks of a data trust is one way of defining the concept itself. To fulfill its consumer-serving mission of preventing certain data flows and enabling others, a data trust must perform various tasks: It must be able to assign access rights to data, it may or may not need to hold data itself, it must be able to audit whether organizations adhere to their agreed conditions and it must have access to credible tools of enforcement.

Providing access to and/or holding data: In the first instance, a data trust must catalog which data each data-generating device and underlying firm(s) collect. This requires a certain level of standardization of data formats. In the smart home, standardizing data formats is a greater challenge for small players, while large players tend to have more resources to convert different formats into one.[20] Based on such a catalog, the data trust must be able to provide access to data as agreed with data-using organizations for the agreed purposes. This often may not require the data trust to hold the data. The data could remain with the data-collecting organizations, or it could reside closer to consumers, as some projects try to implement.[21] Distributed data storage is generally considered preferable, as large, centralized data pools carry a higher security risk. Nevertheless, some data centralization may make sense if the data trust modifies the data before providing access, for example, if the data trust aggregates or anonymizes the data. Data trust pilots may also prefer to hold data if this is easier to implement, such as

20 Various large smart home players have announced to collaborate on a standard for smart home connectivity; see Heater, B., 'Amazon, Apple, Google and Zigbee Join Forces for an Open Smart Home Standard', TechCrunch, 18 December 2019, https://techcrunch.com/2019/12/18/amazon-apple-google-and-zigbee-join-forces-for-an-open-smart-home-standard/.

21 For example, the project "Solid" by Sir Tim Berners-Lee, among others, is developing so-called data pods in which consumers could store their data; see https://solid.inrupt.com/how-it-works.

by combining all smart home data that consumers are willing to provide for energy research.

Auditing and enforcement: It is sensible to expect the data trust to put some effort into ensuring that the trust's agreements are adhered to. Thus, trusts must perform some form of auditing, which is likely to require a combination of technical measures and human involvement.[22] Biobanks, that is, repositories of biological and often genomic material for research purposes, may provide some inspiration for how transparency, certification and auditing can interact to protect highly sensitive data.[23] Where concerns arise about non-compliance with the agreements, it is important that effective enforcement mechanisms are available. Data trusts can sanction organizations, for example, by terminating agreements and withholding data for future use. One way to achieve deterrence would be to consider unauthorized data uses a breach of contract associated with fines or a violation of data protection that can trigger financial sanctions by data-protection authorities.

22 Data Critiques, 'The Challenges of Data Custody & A Testable Plan for Data Trust', 4 July 2019, http://datacritique.com/Data_Trust_RFC.pdf.

23 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, 'Datentreuhänderschaft in der Biobank-Forschung – bdc\Audit, Methoden, Kriterien und Handlungsempfehlungen für die datenschutzrechtliche Auditierung der Datentreuhänderschaft in der Biobank-Forschung', 30 April 2009.

How a data trust could make smart home data accessible for new uses: an example energy use case

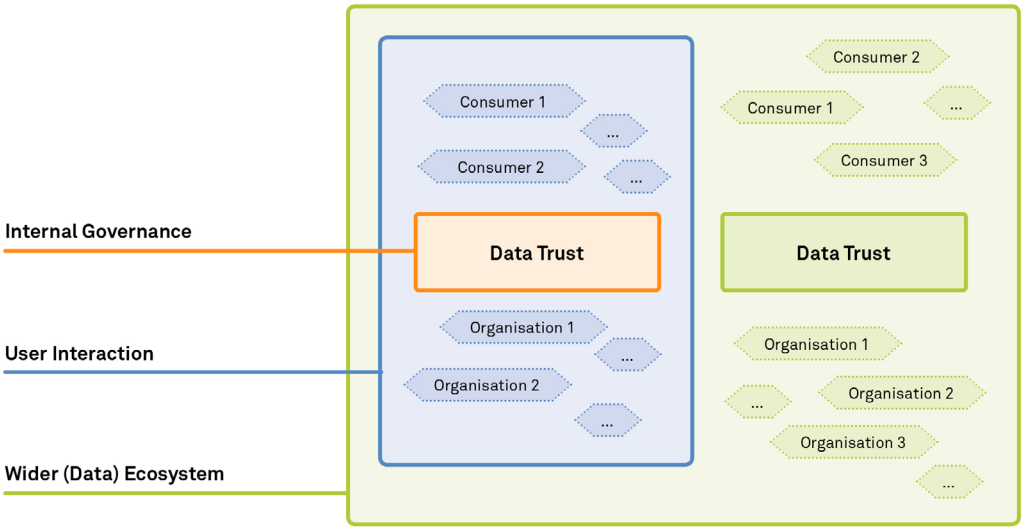
Smart home sensors capture a person's activities in their most personal space, their home. A data trust could allow consumers to select their desired privacy settings in one place for all devices, from smart meters to fridges and TVs. Although many people are likely to consider that data to be sensitive, it also has the potential for useful applications that, for example, could promote energy efficiency:

- Researchers could analyze data on energy usage in the smart home by type of device, time of day and year and other factors that may affect energy consumption, such as weather conditions. This information could allow researchers to assess which part of the energy consumption could be shifted to better match energy production. For example, heating in winter, when a person is at home, is unlikely to be flexible, but the running a washing machine or dishwasher may well be. A data trust could provide researchers access to data that contains only the relevant information, aggregating information across households but not across devices. Such insights could be used to develop recommendations or services to help individuals manage their energy usage in line with production, reducing the overall cost of energy production.
- Consumers may wish to better understand their energy usage patterns and share them with specific parties, for example, alternative energy providers. Consumers currently rely on services provided by their energy service provider that may wish to use the data for purposes such as targeting that individuals do not approve of. A data trust could help consumers move their data across services at the level of granularity required. This could include making data on a household's energy history available to obtain a quote from other energy providers, or data on the energy usage of specific devices to, for example, obtain personalized estimates of the energy consumption of new devices.

3C. A data trust is complex to design

One challenge for the implementation of data trusts is the combination of limited precedent,[24] their consumer-serving mission and their intermediary nature. This combination has led to many questions being raised about the design of data trusts, and more questions are likely to arise in the future. These questions can be grouped into three layers of design, as highlighted in Figure 2. Internal governance describes the inner workings of the trust. User interactions include how the trust interacts with both sides, consumers and organizations. The integration into the wider (data) ecosystem relates to how data trusts interact with other data trusts, as well as with data not governed by data trusts.

Figure 2 – Layers of data trust design



In the following, various questions relating to each layer are listed and three options for addressing them provided. Neither the list of questions nor the answer options are comprehensive, but they are intended to serve as a starting point for a discussion on how to implement data trusts in practice. There is also some interdependence between the layers. For instance, a monopoly data trust is likely to require a much higher level of scrutiny than a competitive data trust ecosystem.

24 Biobanks may serve as a reference point; see Schneider, I. 'Governance der Datenökonomie – Politökonomische Verfügungsmodelle zwischen Markt, Staat, Gemeinschaft und Treuhand', in: Ochs, Carsten with Michael Friedewald, Thomas Hess, and Jörn Lamla (eds.), Die Zukunft der Datenökonomie. Wiesbaden: Springer, 2019, pp. 143-180.

Internal governance

The internal governance of a consumer data trust can take on many different forms, as listed in Table 1. Two questions (shaded in Table 1), funding and the executing organization, are key for making data trusts trustworthy for beneficiaries, that is, the consumers who use a data trust, and are expanded upon in section 4.

Table 1 – Design of internal governance

Characteristic	Option 1	Option 2	Option 3
Funding: how to finance the trust's activities	Commission on data licenses	Public funding	Data-specific taxes
Executing organization: what type of organization can be a data trust	Any kind of organization, including for-profit companies	Non-profit organizations	State-run organizations
Decision-making mechanism: how the trustee makes decisions about data sharing	Majority voting by beneficiaries on individual sharing agreements	Voting of representatives	Aggregation of individual preferences
Default setting: the default regarding data sharing	Opt-in throughout	Consent champions or average of actively chosen settings	Opt-out throughout
Negotiation objectives: what the trustee should maximize in its negotiations with data-using organizations	Income only	Combined utility of income and consumer-friendly data usage	Consumer-friendly data usage only
Data monetization: if the trustee should monetize data	No a allowed	Exemption of sensitive data types from monetization	All data can be monetized
Benefit distribution: how a trustee distributes its benefits among beneficiaries	Dependent on their data contribution	As decided by its beneficiaries	Fully equal
Evaluation: how performance is assessed	Majority voting by members	Optional certification	Mandatory external certification

On decision-making mechanism, see Bunting, Mark, and Suzannah Lansdell, 'Designing Decision-making Processes for Data Trusts: Lessons From Three Pilots', Communication Chambers, April 2019, http://theodi.org/wp-content/uploads/2019/04/General-decision-making-report-Apr-19.pdf.

On consent champions as a tool to determine defaults, see Ruhaak, Anouk, and Josh McKenty, 'Could Consent Champions Help Us Navigate Privacy Concerns?', 24 June 2019, https://www.centerfordigitalcommons.org/privacy/consent/2019/06/24/consent-champions.html.

On data monetization, see Streamr, 'Should We Sell Our Data? A Panel on the Ethics of Individual Data Monetisation', YouTube, 31 October 2019, https://www.youtube.com/watch?v=6ni9K0JjI-k.

On evaluation, see Bunting and Lansdell (2019, above) and Martin, Sabrina, and Walter Pasquarelli, 'Exploring Data Trust Certification', Oxford Insights, April 2019, http://theodi.org/wp-content/uploads/2019/04/Report_-Exploring-Data-Trust-Certification.pdf.

The other questions also concern how a trust is made accountable vis-à-vis its beneficiaries. Different decision-making mechanisms can be envisaged to link the trustee's decisions to its beneficiaries' preferences. A default setting is needed in particular if consumers are nudged or even obliged to join a trust, which, in turn, may be necessary to make sure the most vulnerable are protected by a trust (see the following sub-section). The default could take on one of the two "extremes," opt-in or opt-out throughout, or a middle ground. A data trust must decide what it wants to maximize; if data monetization is deemed acceptable, a trade-off between monetary compensation and other forms of consumer benefits is likely to arise. For these benefits, the trust also must decide how to distribute them among its beneficiaries: Making their share dependent on their data-sharing settings may provide a too strong incentive to share data, while a fully equal distribution could lead to under-sharing and free-riding if beneficiaries wish to reap the benefits of data shared by others. Last, different mechanisms can help assess whether the trust is fulfilling its purpose, using internal and/or external reviews of the trust's work.

User interaction

The trust's interaction with its users is important to ensure that data flows from consumers to organizations are effective in benefiting consumers. Two questions (shaded in Table 2), the discretionary space that consumers can give a trust and accessibility for organizations, are key for making data trusts easy to use for their beneficiaries, and are expanded upon in section 4.

Table 2 – Design of user interaction

Characteristic	Option 1	Option 2	Option 3
Discretionary space: to what extent consumers can delegate their data decisions to a trust	High consumer involvement	Level of involvement chosen by consumer	Low consumer involvement
Accessibility for organizations: how organizations can get access to data through a trust	High barriers to access, especially in comparison with other access options	Some barriers to access, including concluded negotiations and transparency requirements	No barriers to access
Joining mechanism for consumers: how consumers sign up for a data trust	Fully optional	Public encouragement	Mandatory sign-up

On joining mechanism for organizations, see London Economics, 'Independent Assessment of the Open Data Institute's Work on Data Trusts and on the Concept Of Data Trusts', April 2019, http://theodi.org/wp-content/uploads/2019/04/Datatrusts-economicfunction.pdf.

Characteristic	Option 1	Option 2	Option 3
Openness of trusts: if trusts can decide to reject beneficiaries	No	Yes, but only for specific reasons	Yes
Joining mechanism for organizations: how organizations use a data trust	Fully optional	Encouraged usage, e.g., through taxation	Mandatory usage
Negotiation rules: how trustees can negotiate with organizations	No rules	Some rules, e.g., to prevent discrimination of small organizations	Fully specified framework
Creation of trusts: how trusts can be set up	By consumers	By a supervisory body	By organizations

In addition, a data trust can have different ways of interacting with consumers: Consumers may be free to choose a data trust as an alternative to direct interactions with data-using organizations, or regulation may require consumers to choose a data trust, similar to how consumers in many countries must buy health insurance. Data trusts may wish to reject beneficiary applications, for example, if the existing beneficiaries believe new beneficiaries would reap more than they contribute. Such rejections may or may not be acceptable, and could require regulation. For organizations, using data through a data trust may be optional or could be stipulated through regulatory measures. It may be desirable to impose some rules on how trusts negotiate with organizations, for example, to prevent trusts from making more demanding claims on small organizations vis-à-vis the trust has more bargaining power than vis-à-vis large organizations.

Market structure

The integration of data trusts into the wider data ecosystem, including other data trusts and data held outside data trusts, is likely to become more of a concern as they become more widely used. Nonetheless, it is useful to be aware of these questions to make sure decisions about data trust design do not imply potentially undesirable answers to questions about the wider market design.

Table 3 – Design of market structure

Characteristic	Option 1	Option 2	Option 3
Horizontal concentration: if data trusts should compete for users	Monopoly data trust	A supervised number of data trusts	Full competition
Domain-specific specialization: what types of data a trust should hold	Narrow: limited to one type of data	Broad: covering all data in one domain	Comprehensive: covering data from all domains
Interaction with external data: how to deal with data outside data trusts	Mandatory integration into data trusts	Mandated priority of data from data trusts	Free use of external data

The first two questions are about a data trust's scope, in horizontal and vertical dimensions. Competition between data trusts that oversee the same type of data may be desirable to ensure that the trusts offer a broad enough choice to consumers and are innovative. However, the network effects between organizations and consumers may favor concentration or even a monopoly data trust, as this type is more likely to be able to provide access to large and valuable datasets. Similarly, data trusts may serve specific purposes, such as providing access to data on energy-usage patterns in a small region. A narrow set-up would make it easier to link the trust's activities to a specific purpose and community, but would require consumers to sign up to many trusts in parallel. At the other end of the spectrum, one data trust or only a few could cover data of all types, including the smart home, mobility, health, entertainment and consumption habits. A broad set-up is likely to be more efficient, but much harder to oversee. Horizontally and vertically, data trusts may need to deal with overlapping data, for example, where household members have different data-sharing preferences regarding their smart home data, or where smart home data is relevant for health as well. Last, the relationship between the data within and outside data trusts will require clarification: Organizations may be free to use external data, potentially undermining the data trust's effectiveness, or they may be required to use data from data trusts.

4. The three most pressing challenges for implementation

Data trusts raise various questions about their design. However, not all of these questions are equally urgent to answer, as the primary objective is to turn data trusts from an academic concept into a data-sharing mechanism the usefulness of which can be assessed in practice. Three imminent challenges prevent data trusts from being implemented:

- Aligning interests: How can we make sure that the interests of the trust are aligned with those of the individuals it represents?
- Delegating consent: How can we make it easy for consumers to express their interests?
- Enabling innovation: How can organizations be motivated to work with data trusts?

Consumer trusts would act as intermediaries between organizations and consumers with indirect network effects: Data trusts will be more appealing to organizations if the trusts represent many consumers, and consumers may be more inclined to join a data trust if the trust can negotiate effectively with many organizations. Thus, consumers and organizations must accept the data trust to turn it into a viable business model. The first two challenges deal with the consumer side, and why current approaches have not gained more traction. First, data trusts tend to require too much effort to use, a problem that has plagued many systems for personal information management. Second, trust is key, and where organizations aim to portray themselves as data trusts concerns about potential conflicts of interest arise. Third, data trusts must enable consumer-friendly data uses to deliver functionality over and above what could be achieved with stricter regulation. Using data in line with consumers' interests may stimulate new business models and more data-driven economic activity.

4A. Aligning interests: How do we build trust?

Consumers put a high value on the trustworthiness of data-using organizations, but express distrust about most organizations that use data about individuals.[25] Thus, the data trust must be set up to ensure that the trust's in-

25 Open Data Institute, 'Who Do We Trust With Personal Data?', 5 July 2018, https://theodi.org/article/who-do-we-trust-with-personal-data-odi-commissioned-survey-reveals-most-and-least-trusted-sectors-across-europe/.

terests are aligned with those of consumers and that any potential conflicts of interest are resolved in favor of consumers. This alignment should be reflected in the legal set-up of the trust that reflects some form of fiduciary duty of the trust toward its beneficiaries, consumers. It could take the form of a legal trust under English law,[26] a German "Stiftung" or a data foundation under Channel Island law,[27] or contracts may suffice to align interests.[28] In any case, consumers must be able to understand and verify the trust's activities, for example, with the help of certification.[29] Organizations such as CoreTrustSeal[30] provide a starting point to make sure data trusts comply with good data storage practices.

The funding of the trust's activities is often mentioned as a potential source of conflicts of interest. Pure public funding is problematic, as it could give the state powers to demand access to more data than would be in consumers', in this context, citizens', interest. Setting up the fund with for-profit objectives is likely to be problematic as it may incentivize data-sharing for the highest price, not for the largest benefit for consumers. However, there are ways in which data trusts could be funded that are compatible with their consumer-oriented mission:

- **initial funding from public sources:** Given the benefit expected for wider society, there is a case for some public funding. It could cover costs associated with setting up a data trust at the beginning, such as investments into technology and overhead. To avoid long-term dependency on political goodwill, then the public funding should be phased out.

- **data tax or levy:** Correlated data implies that much of current data trading creates negative externalities. This provides a rationale for a tax on

26 See e.g. Delacroix and Lawrence (2019, fn 21).

27 Stalla-Bourdillon, Sophie, Alexsis Wintour, and Laura Carmichael, 'Building Trust Through Data Foundations, a Call for a Data Governance Model to Support Trustworthy Data Sharing', December 2019, https://cdn.southampton.ac.uk/assets/imported/transforms/content-block/UsefulDownloads_Download/69C60B6AAC8C4404BB179EAFB71942C0/White%20Paper%202.pdf.

28 Queen Mary University of London, BPE Solicitors LLP, and Pinsent Masons LLP, 'Data Trusts: Legal and Governance Considerations', April 2019, http://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf

29 Martin and Pasquarelli (2019, see note to Table 1).

30 https://www.coretrustseal.org/

data trading.[31] A tax could be imposed specifically on trades that happen outside data trusts, or come in the form of a levy on data-generating devices, such as smart meters. Although internalizing some of the negative effects, such measures could also provide funding for a data trust. To avoid perverse incentives, the data trust should have no direct influence on that trading activity or sales of data-generating devices.

- **membership fee funded through data sales:** Assuming the data trust negotiates payments for some of the licenses to data-using organizations, a contribution could be given to the data trust. This membership fee should be low enough that it does not incentivize the trust to engage in excessive trading, and the fee should be a fixed amount, that is, not a percentage of data-related revenue.

A combination of these funding options, and potentially other sources, can allow a trust to negotiate on behalf of consumers without a conflict of interests.

4B. Delegating consent: How to ensure consumer usability?

Consumers put a high value on the usability of services, and convenience is an important driver of their uptake. Reducing the number of clicks required, or rankings can have a significant impact on consumer behavior.[32] Thus, for consumers to perceive a data trust as a service that creates a tangible benefit for them, the trust must reduce the unmanageable burden of information and engagement in decisions that consumers are willing and able to make. Such decisions could be made, for example, by asking consumers to indicate their preferences regarding different types of data and different data uses, or by giving consumers the option to follow the preferences of a person or institution they trust.[33]

31 The design of such a tax, in turn, should be based on evidence that is likely to become available as data trusts are set up. As some researchers have pointed out, there is a possibility for taxes to reduce social welfare as they may prevent beneficial data exchanges. See Acemoglu, D., A. Makhdoumi, A. Malekian, and A. Ozdaglar, 'Too Much Data: Prices and Inefficiencies in Data Markets', NBER Working Paper No. 26296, 2019.

32 Whether privacy-friendly products appear first or second on a list can affect their uptake significantly. See e.g. Athey, Susan C., Christian Catalini, and Catherine E. Tucker, 'The Digital Privacy Paradox: Small Money, Small Costs, Small Talk', Stanford University Graduate School of Business Research Paper No. 17-14, 8 April 2018.

33 Ruhaak and McKenty (2019, see note to Table 1).

Delegation of consent and the rights to data access and portability may not be fully compatible with current rules under the GDPR. Data can be processed based on "consent" (Articles 6.1a and 7 GDPR), which has led to the proliferation of online banners asking consumers to confirm their desired cookie settings. Such consent must be specific to clearly named purposes. Only in the context of scientific research can consent be given for broader purposes (Recital 33). An explicit provision for representation on a consumer's behalf is made only for complaint proceedings (Article 80).
Some legal experts believe that representation for the purpose of consent is feasible in principle, but there is no legal certainty about how closely involved the represented consumers should remain. In any case, broad representation is not deemed feasible. Especially in the smart home, where a large part of the collected data may provide insights into the health of individuals, requirements for consent are higher. These requirements make it more difficult to set up meaningful representation, but continue to put the burden of information, negotiation and understanding of the wider social impact on individuals. Thus, the current legal framework may inadvertently sustain the market failures that prevent consumers from asserting their interests in how data about them is used.

If a data trust is to deliver benefits to consumers, it must be usable. To be user-friendly, data trusts must give consumers the option of delegating consent and (some of) their rights. There are at least two ways to implement this. One option is to extend the possibility for representation (Article 80) to include exercising data rights, including the rights to access, port and erase data. Another option is to allow consumers to delegate (the right to provide) consent and the right to withdraw consent. In this case, it could make sense to, for example, assign data trusts a privileged status. This would ensure that only organizations that comply with certain standards, possibly certification and financing requirements (see section 4A), represent consumers.

4C. Enabling innovation: What is in it for organizations?

If data trusts are to create benefits for consumers, organizations also should use the trusts. This may be achieved through incentives or might require regulation in some cases. In any case, data trusts should be designed to enable organizations to use data in line with consumers' interests. For this to happen, organizations must be able to access data through data trusts easily, provided the organizations demonstrate that their data uses do not conflict with consumers' interests (e.g., the data is used for the development of pro-

ducts that many consumers demand). The prospect of access to more data may be enough for many organizations, in particular, small companies, to engage with a data trust. If the data trust can help spread the value of data more widely than currently is the case, organizations may find it easier to innovate for the benefit of consumers.

Such a use of data trusts could even lead to a paradigm shift away from the current understanding which emphasizes the amount of data collected, where less data is understood to be more consumer-friendly. A different understanding could focus on the uses to which the data is put: Using more data can be more consumer-friendly if the data-driven services work for the benefit of consumers. For example, a data trust could license smart speaker data to device producers where this is in line with the consumers' general privacy preferences, leading to more data being shared than if consumers must opt in. The data trust could negotiate certain safeguards that otherwise may not be in place (such as a requirement for a device to indicate when it is recording, that the data should not be used for profiling, etc.).

5. The way forward: testing small before scaling up

Considering the wide endorsement that data trusts have received, the lack of practical implementation is surprising. The intermediary nature of data trusts means that many decisions must be made about their design. However, if the motivation to try out new forms of data governance is great enough (and the current political climate suggests it may be), it should be possible to test whether and how data trusts can live up to their expectations. To do so, it is important to solve the imminent challenges first and be willing to test and learn about how to best resolve the remaining open questions for the design of a data trust. A data trust must be trustworthy and easy to use from a consumer perspective, as well as provide data-using organizations with a negotiating partner for access to sufficiently large quantities of data.

Given that consumers are the designated beneficiaries of data trusts described in this paper, only real-world projects can help determine where data trusts can deliver significant benefits, and how the trusts should be designed for that purpose. Pilots and experiments, combined with wider engagement, are likely to deliver the most reliable results and provide real-world behavioral insights into how consumers and organizations use data trusts. Only once there is sufficient evidence available on how consumers respond to different designs of data trusts in different contexts should further steps be considered. These steps may be necessary to help data trusts scale up and to ensure their intended use is not undermined: for example, guidelines for the design of data trusts, strict certification requirements or legislation extending the scope of their agreements beyond those who actively sign up to a data trust. This may be necessary to make sure the benefits of data trusts do not reach only the least vulnerable consumers and do not arise only from interactions with organizations whose interests are most aligned with those of consumers anyway.

Collecting this evidence may be difficult in the current legal framework that does not allow for a sufficiently broad delegation of consent and data rights to a trusted entity. Trying out alternative ways of ensuring data use in the interest of consumers would complement the ongoing efforts to enforce the GDPR. Given that the GDPR legislation is unlikely to be subject to substantive change soon, regulatory sandboxes could provide a safe space for testing such changes and the impact of data trusts. The United Kingdom has tested the approach in different industries: The Financial Conduct Authority allows companies to test new products with real customers on a limited scale under

close supervision by the authority.[34] The Information Commissioner's Office has also started working with the first cohort of companies that can test innovative forms of data use while receiving advice on compliance.[35] This would also allow for testing if, and if so, how, existing legislation should be adjusted to enable effective data trusts.

Another challenge, but also an opportunity, is the decision about where to start. The smart home can be an interesting testing ground because its data exhibits two key features that data trusts may be able to address better than other approaches. The data is highly personal as it relates to people's lives in their private space, their home. However, the data has great potential when used and combined, for example, to reduce energy consumption, to reduce the burden of housework or to assist vulnerable groups in living independently. Thus, striking a balance between preventing undesirable data uses and enabling beneficial ones is an important challenge that data trusts may help solve. However, performing multiple pilots, in the beginning, in multiple areas is useful. This would help explore on a small scale how to best design data trusts.

34 Financial Conduct Authority, 'Regulatory Sandbox', https://www.fca.org.uk/firms/innovation/regulatory-sandbox.

35 Information Commissioner's Office, 'Sandbox Beta Phase, Discussion Paper', https://ico.org.uk/media/about-the-ico/documents/2614219/sandbox-discussion-paper-20190130.pdf

Acknowledgements

I am very grateful to those who have provided input and comments and/or participated in a workshop, including Guido Brinkel, Microsoft, Eileen Fuchs, Bundesministerium des Innern, für Bau und Heimat, Wolfgang Kerber, Universität Marburg, Beatrix Reiß, comuny, Frederick Richter, Stiftung Datenschutz, Ingrid Schneider, Universität Hamburg, Christian Thorun, ConPolicy and many more. Thanks also go to the SNV team for their support, in particular Stefan Heumann, Jan-Peter Kleinhans and Fintan Viebahn.

Bibliography

Acemoglu, D., A. Makhdoumi, A. Malekian, and A. Ozdaglar, 'Too Much Data: Prices and Inefficiencies in Data Markets', NBER Working Paper No. 26296, 2019.

Acquisti, Alessandro, Leslie K. John, and George Loewenstein, 'What Is Privacy Worth?,' The Journal of Legal Studies, 42(2), June 2013, pp. 249-274.

Amazon, 'Alexa and Alexa Device FAQs', https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230.

Ambulanzpartner, 'Note of Thanks for Data Donation for an Important Publication on the Treatment of Spasticity in ALS', Ambulanzpartner, 5 December 2019, https://www.ambulanzpartner.de/note-of-thanks-for-data-donation-for-an-important-publication-on-the-treatment-of-spasticity-in-als/?lang=en.

Athey, Susan C., Christian Catalini, and Catherine E. Tucker, 'The Digital Privacy Paradox: Small Money, Small Costs, Small Talk', Stanford University Graduate School of Business Research Paper No. 17-14, 8 April 2018.

Bergemann, Dirk, Alessandro Bonatti, and Tan Gan, 'The Economics of Social Data', Cowles Foundation Discussion Paper No. 2203, 25 September 2019; Choi, J. P., D. S. Jeon, and B. C. Kim, 'Privacy and Personal Data Collection With Information Externalities', Journal of Public Economics, 173, 2019, pp. 113-124.

Bundesministerium für Wirtschaft und Energie (2020), 'Entwurf eines Zehnten Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0'.

Bunting, Mark, and Suzannah Lansdell, 'Designing Decision-making Processes for Data Trusts: Lessons From Three Pilots', Communication Chambers, April 2019, http://theodi.org/wp-content/uploads/2019/04/General-decision-making-report-Apr-19.pdf.

Campbell, James David, Avi Goldfarb, and Catherine E. Tucker, 'Privacy Regulation and Market Structure', Journal of Economics & Management Strategy, 24(1), 2015, pp. 47-73.

Common Voice, Mozilla Initiative, https://voice.mozilla.org.

Competition and Markets Authority, 'Online Platforms and Digital Advertising Market Study,

Interim Report', December 2019. Data Critiques, 'The Challenges of Data Custody & A Testable Plan for Data Trust', 4 July 2019, http://datacritique.com/Data_Trust_RFC.pdf.

Datenethikkommission der Bundesregierung, 'Gutachten der Datenethikkommission', Potsdam, Bundesministerium des Innern, für Bau und Heimat, 2019, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=5.

Day, Matt, Giles Turner and Natalia Drozdiak, 'Amazon Workers Are Listening to What You Tell Alexa', Bloomberg, 11 April 2019, https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio.

Delacroix, Sylvie, and Neil D. Lawrence, 'Bottom-up Data Trusts: Disturbing the "One Size Fits All" Approach to Data Governance', International Data Privacy Law, ipz014, 2019.

Deloitte, 'Smart Home Consumer Survey 2018: Ausgewählte Ergebnisse für den deutschen Markt', Deloitte, May 2018, https://www2.deloitte.com/content/dam/Deloitte/de/Documents/technology-media-telecommunications/Deloitte_TMT_Smart_Home_Studie_18.pdf.

Financial Conduct Authority, 'Regulatory Sandbox', https://www.fca.org.uk/firms/innovation/regulatory-sandbox.

Hall, Dame Wendy and Jérôme Pesenti, 'Growing the Artificial Intelligence Industry in the UK', Department for Digital, Culture, Media & Sport and Department for Business, Energy & Industrial Strategy, 15 October 2017, Recommendations of the Review, https://www.gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk/recommendations-of-the-review.

Hardinges, Jack, Peter Wells, Alex Blandford, Jeni Tennison, and Anna Scott, 'Data Trusts: Lessons From Three Pilots', Open Data Institute, April 2019, https://docs.google.com/document/d/118RqyUAWP3WIyyCO4iLUT3oOobnYJ-GibEhspr2v87jg/edit.

Heater, B., 'Amazon, Apple, Google and Zigbee Join Forces for an Open Smart Home Standard', TechCrunch, 18 December 2019, https://techcrunch.com/2019/12/18/amazon-apple-google-and-zigbee-join-forces-for-an-open-smart-home-standard/.

Husseini, T., 'As Energy Companies Race to Cash in on Data, Should We Be

Worried?', Power Technology, 31 July 2018, https://www.power-technology.com/features/energy-companies-sharing-data/.

Information Commissioner's Office, 'Sandbox Beta Phase, Discussion Paper', https://ico.org.uk/media/about-the-ico/documents/2614219/sandbox-discussion-paper-20190130.pdf.

Jentzsch, Nicola, 'Die persönliche Datenökonomie: Plattformen, Datentresore und persönliche Clouds', Deutsches Institut für Wirtschaftsforschung, 31 January 2017, https://stiftungdatenschutz.org/fileadmin/Redaktion/Bilder/Abschluss_Studie_30032017/stiftungdatenschutz_Gutachten_Die_persoenliche_Datenoekonomie_Anhang_2_final.pdf.

John, Leslie K., Alessandro Acquisti, and George Loewenstein, 'Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information', Journal of Consumer Research, 37(5), 2010, pp. 858-873.

Kettner, Sara Elisa, Christian Thorun, and Jan-Peter Kleinhans, 'Big Data im Bereich Heim und Freizeit Smart Living: Status Quo und Entwicklungstendenzen', ABIDA - Assessing Big Data, German Federal Ministry of Education and Research, 2018, https://www.abida.de/sites/default/files/Gutachten_HeimUndFreizeit.pdf.

Khalilzadeh, Ebrahim, 'We've Open-sourced Swash to Make Data Unions a Reality', Medium, 9 December 2019, https://medium.com/swashapp/weve-open-sourced-swash-to-make-data-unions-a-reality-7049e92c364b.

Kommission Wettbewerbsrecht 4.0, 'Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft: Bericht der Kommission Wettbewerbsrecht 4.0', German Federal Ministry for Economic Affairs and Energy, September 2019,

https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/bericht-der-kommission-wettbewerbsrecht-4-0.pdf?__blob=publicationFile&v=10.

Libert, Timothy, Lucas Graves, and Rasmus Kleis Nielsen, 'Changes in Third-Party Content on European News Websites after GDPR', August 2018, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2018-08/Changes%20in%20Third-Party%20Content%20on%20European%20News%20Websites%20after%20GDPR_0_0.pdf.

London Economics, 'Independent Assessment of the Open Data Institute's Work on Data Trusts and on the Concept Of Data Trusts', April 2019, http://theodi.org/wp-content/uploads/2019/04/Datatrusts-economicfunction.pdf.

Mantelero, A., 'Personal Data For Decisional Purposes in the Age of Analytics:

From an Individual to a Collective Dimension of Data Protection', Computer Law & Security Review, 32(2), 2016, pp. 238-255.

Martin, Sabrina, and Walter Pasquarelli, 'Exploring Data Trust Certification', Oxford Insights, April 2019, http://theodi.org/wp-content/uploads/2019/04/Report_-Exploring-Data-Trust-Certification.pdf.

Open Data Institute, 'Who Do We Trust With Personal Data?', 5 July 2018, https://theodi.org/article/who-do-we-trust-with-personal-data-odi-commissioned-survey-reveals-most-and-least-trusted-sectors-across-europe/.

Queen Mary University of London, BPE Solicitors LLP, and Pinsent Masons LLP, 'Data Trusts: Legal and Governance Considerations', April 2019, http://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf

Ruhaak, Anouk, 'Data Trusts: Why, What and How', Medium, 12 November 2019, https://medium.com/@anoukruhaak/data-trusts-why-what-and-how-a8b53b53d34.

Ruhaak, Anouk, and Josh McKenty, 'Could Consent Champions Help Us Navigate Privacy Concerns?', 24 June 2019, https://www.centerfordigitalcommons.org/privacy/consent/2019/06/24/consent-champions.html.

Samson, Renate, Kayshani Gibbon, and Anna Scott, 'About Data about Us', Open Data Institute, the RSA (Royal Society for the Encouragement of Arts, Manufacturers and Commerce), and Luminate, September 2019, https://www.thersa.org/globalassets/pdfs/reports/data-about-us-final-report.pdf.

Scheuer, Stefan, and Dietmar Neuerer, 'Der Sprachassistent der Telekom soll Amazon herausfordern – Experten bemängeln Datenschutz', Handelsblatt, 22 October 2019, https://www.handelsblatt.com/technik/it-internet/hallo-magenta-der-sprachassistent-der-telekom-soll-amazon-herausfordern-experten-bemaengeln-datenschutz/25141186.html.

Schneider, Ingrid, 'Governance der Datenökonomie – Politökonomische Verfügungsmodelle zwischen Markt, Staat, Gemeinschaft und Treuhand', in: Ochs, Carsten with Michael Friedewald, Thomas Hess, and Jörn Lamla (eds.), Die Zukunft der Datenökonomie. Wiesbaden: Springer, 2019, pp. 143-180.

Stalla-Bourdillon, Sophie, Alexsis Wintour, and Laura Carmichael, 'Building Trust Through Data Foundations, a Call for a Data Governance Model to Support Trustworthy Data Sharing', December 2019, https://cdn.southampton.ac.uk/assets/imported/transforms/content-block/UsefulDownloads_Download/69C60B6AAC8C4404BB179EAFB71942C0/White%20Paper%202.pdf.

Streamr, 'Should We Sell Our Data? A Panel on the Ethics of Individual Data Monetisation', YouTube, 31 October 2019, https://www.youtube.com/watch?-v=6ni9K0JjI-k.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, 'Datentreuhänderschaft in der Biobank-Forschung – bdc\Audit, Methoden, Kriterien und Handlungsempfehlungen für die datenschutzrechtliche Auditierung der Datentreuhänderschaft in der Biobank-Forschung', 30 April 2009.

vom Hofe, Klaus, 'Privacy Bots: Telekom prämiert Ideen', Telekom, 26 July 2017, https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/archiv-datenschutznews/news/privacy-bots-telekom-praemiert-ideen-499988.

World Economic Forum, 'Rethinking Personal Data: Trust and Context in User-Centred Data Ecosystems', Geneva, Switzerland: World Economic Forum, May 2014, http://www3.weforum.org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014.pdf.

Zuiderveen Borgesius, Frederik, Sanne Kruikemeier, Sophie Boerman, and Natali Helberger, 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation', European Data Protection Law Review, 3(3), 15 March 2018, pp. 353-368.

Über die Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Neue Technologien verändern Gesellschaft. Dafür brauchen wir rechtzeitig politische Antworten. Die Stiftung Neue Verantwortung ist eine unabhängige Denkfabrik, in der konkrete Ideen für die aktuellen Herausforderungen des technologischen Wandels entstehen. Um Politik mit Vorschlägen zu unterstützen, führen unsere Expertinnen und Experten Wissen aus Wirtschaft, Wissenschaft, Verwaltung und Zivilgesellschaft zusammen und prüfen Ideen radikal.

Über die Autorin

Aline Blankertz leitet das Projekt „Datenökonomie“, das ökonomische, technische und gesellschaftliche Fragestellungen untersucht, um innovative datenpolitische Handlungsempfehlungen zu entwickeln. Vor der Stiftung Neue Verantwortung leitete sie verschiedene wirtschaftswissenschaftliche Analysen zur Plattformökonomie, darunter zu Wettbewerb, Datenschutz und Algorithmen.

So erreichen Sie die Autorin

Aline Blankertz
Projektleiterin Datenökonomie
ablankertz@stiftung-nv.de
+49 (0)30 40 36 76 98 1

Impressum

Stiftung Neue Verantwortung e. V.

Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Jan Kloethe

Free Download:

www.stiftung-nv.de