moz://a

Is that even legal?

A guide for builders experimenting with data governance in the **United States**

February 2023

By Beatriz Botero Arcila

with the collaboration of Teodora Groza and Peter McCarthy

About Mozilla

Mozilla's mission is to ensure the internet is a global public resource, open and accessible to all. An internet that truly puts people first, where individuals can shape their own experience and are powerful, safe, and independent.

Founded as a community open source project in 1998, Mozilla currently consists of two organizations: the nonprofit Mozilla Foundation, which leads our movement building work; and its wholly owned subsidiary, the Mozilla Corporation, which leads our market-based work, including the development of the Firefox web browser. The two organizations work in close concert with each other and a global community of tens of thousands of volunteers under a single banner: Mozilla.

Acknowledgements

The author wishes to thank Giovanna Hajdu Hungria da Custódia for excellent editorial assistance and research assistance. We would further like to thank Stefan Baack, Lisa Gutermuth, Solana Larsen, and Kasia Odrozek, who provided valuable feedback on this work. We also thank Kristina Shu and Nancy Tran from Mozilla Foundation's design team for their support in designing this report. Ran Zheng created the illustrations you'll find throughout these pages. Thanks are further due to J. Bob Alotta, Champika Fernando, Mehan Jayasuriya, EM Lewis-Jong, Jackie Lu, Anouk Ruhaak, Udbhav Tiwari, and Richard Whitt for informing the direction of this project.

This work was led by Mozilla's Insights team. Eeva Moore led design and engagement work, Kenrya Rankin edited the research, and Neha Ravella provided project management support. Maximilian Gahntz was the project lead.

Disclaimer

The content of this report does not constitute legal advice. Please seek the advice of a qualified attorney.

Table of Contents

Preface

By Mozilla Insights

It's a long-established fact: today's data economy is not built on a level playing field. The people and communities whose data form its lifeblood are fighting to retain or regain control over their data and the value created from it. All too often, data is extracted and processed far removed from its source, serving the interests of the organizations that collect it rather than the people it impacts. This is why it's important to explore new ways to govern data: to shift control, strengthen agency, to share value. Through the Mozilla Foundation's Data Futures Lab and our work around data governance, we are working to challenge this current paradigm.

Reimagining, reconstituting, and rebalancing data governance requires system-level change, but opportunities to implement new ideas for better data governance often also exist within existing paradigms and legal frameworks. Just as the open source movement challenged copyright laws to introduce open licensing decades ago, builders can similarly defy existing laws and regulations to push the boundaries of how data is governed. Builders can shape new norms by leveraging opportunities present in existing rules. But to do so, they need a firm understanding of current realities. We aim to help them navigate existing legal landscapes so they can help pave the way for better data governance models and policy in the future.

The primary goal of this research is therefore twofold:

- To provide builders with an overview of the current (and changing) legal landscape governing the collection, management, sharing, and use of data in their country;
- to identify opportunities for what we call "alternative data governance" models within existing legal landscapes — specifically, where the regulatory status quo offers pathways to implement new approaches that shift power from data collectors to data subjects — that create meaningful incentives for the benefits of data to be shared between various parties and enable data to serve individual or collective interests.

The guiding question is: What can be built where, and using which levers, from a legal standpoint?

The analysis in this guide will provide builders with a map of laws and regulations relating to data and opportunities for experimentation. It will also provide concrete dos and don'ts for builders experimenting with new approaches to data governance.

Overview

This report starts with an overview of laws and regulations — and, to a certain extent, a lack thereof — governing data in the United States before presenting emerging approaches to data governance in three case studies: one on data collaboratives, another on trustworthy intermediaries, and a third on data cooperatives (or co-ops).

First, the report discusses the legal landscape relating to data in the U.S. In the absence of a comprehensive federal data protection law, a self-regulatory approach focused on notice and choice has become the dominant approach to data governance. Additionally, this overview covers sectoral data governance rules — for example in the financial and healthcare sectors — and rules passed at the state level (notably in California, Colorado, Connecticut, Virginia, and Utah).

In the first case study, the report explores the potential of data collaboratives, specifically in the context of corporate risk management. Data collaboratives can facilitate the sharing and pooling of data between participants to unlock its collective value. This can be particularly helpful in sectors where data is available, but not shared and where data sharing doesn't create competitive disadvantages. The report then discusses the concept of trustworthy intermediaries. Inspired by trust law — under which trustees manage certain assets based on a fiduciary duty they owe to a beneficiary — the idea of trustworthy intermediaries is to help people exercise more control over their data by compelling the intermediary to manage said data in their interest.

In the final case study, the report discusses data co-ops. Data co-ops are membership-based, collectively owned, and democratically governed organizations that serve the interests of their members. They are meant to collect, manage, and leverage members' (and potentially others') data, for example to empower gig workers vis-à-vis labor platforms.

How to read this guide

Throughout this report, you will find a number of recurring elements that make it easy to find exactly what you're looking for. The result is a reference that does not need to be read from cover to cover in a linear way; you can simply dip in and out of different sections as needed. The recurring elements are:

- Brief summary boxes of key themes and findings from each section.
- Case studies that dive deep into specific approaches to data governance, compete with additional resources to extend your knowledge.
- Checklists of concrete steps that may help you in your journey.

Additionally, the report contains a glossary with brief explanations of specific concepts and legal texts.

What this guide does *not* include is legal advice. It rather aims to provide a starting point in your exploration of this topic to help you ask the right questions and identify areas where bespoke advice from lawyers is necessary.

Overview of the legal landscape

In this section:

- There is no single, comprehensive federal law regulating how companies and the government collect, store, and share personal data in the United States.
- In the private sector, the main regime is notice and choice, a self-regulatory approach that invites private companies to adopt self-binding privacy policies.
- A few sectors have specific rules for certain types of institutions given the sensitivity of the data they collect. This is the case for the financial sector, much of the health care sector, email, telecoms, and content for children.
- Similarly, several states, notably California, have enacted (or are planning to enact) comprehensive privacy rules that give users more control over their personal data. These rules apply to everyone doing business within their jurisdiction.
- The government is bound by the Fourth Amendment, which requires that, in most situations, the government must have a warrant to access personal and privately held data.
- Once you give personal data away, you lose those personal guarantees and the data can be further shared to third parties — this is known as the third-party doctrine.
- The third-party doctrine and the notice and choice regime have enabled the rise of a significant market for personal data, as legally collected data can be shared or sold downstream with few constraints. The data market, though providing significant convenience for consumers and opportunity for companies, also represents an important surveillance risk for individuals.
- The current legal regime is flexible enough for builders to be creative in building structures that uphold data subjects' interests. Data collaboratives, data trusts, and data co-ops are all intermediary bodies or entities that pool data and create an intermediary structure that enables data sharing, democratizes insights, or embeds mechanisms for users to have more control over how data is used.

No single, comprehensive federal law regulates how companies collect, store, or share customer data in the United States. It is rather a fragmented body composed of constitutional protections, federal and state statutes, torts, regulatory rules and treaties, and self-regulation by companies. The closest to a baseline personal data governance law that exists in the U.S. is the Federal Trade Commission Act of 1914, Section 5, which since 1938 outlawed "unfair or deceptive acts or practices" in commerce.[1] Following this mandate, the Federal Trade Commission (FTC) enforces companies' privacy policies on companies.[2]

Though many domains of law are relevant in data governance, three main bodies of law govern data in the United States: privacy law, intellectual property law, and antitrust and competition law. The analysis that follows concentrates on those bodies of law, what might come next, and how they can be best used by builders to employ alternative data governance in their own projects.

Self-regulation and notice and choice

Companies have written privacy policies (or "notice and choice" documents) — in which they describe the various ways they collect, use, and share users' personal information — since the early days of the commercial internet. These privacy policies stem from the Fair Information Practice Principles (FIPP), first stated in 1973 in a report by the U.S. Department of Health, Education, and Welfare, and restated and expanded in the OECD Guidelines of 1980.[3] [4] One of the most prominent FIPP is the individual right to be given notice about the data gathered about oneself and the right to know how it will be used. Another main FIPP is the individual right to consent to the collection and use of personal data.[5]

Privacy policies were introduced as a largely voluntary measure adopted by companies on the internet to promote their privacy practices and to promote a self-regulatory

---

[1] U.S. Federal Trade Commission Act of 1914, Section 5.

[2] Solove, Daniel J. and Hartzog, Woodrow, "The FTC and the New Common Law of Privacy" (August 15, 2013). 114 Columbia Law Review 583 (2014), GWU Legal Studies Research Paper No. 2013-120, GWU Law School Public Law Research Paper No. 2013-120, Available at SSRN: https://ssrn.com/abstract=2312913 or http://dx.doi.org/10.2139/ssrn.2312913.

[3] U.S. Department of Health, Education and Welfare, "Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems," 41–42. 1973, https://epic.org/documents/hew1973report/.

[4] Ministerial Council of the Org. for Econ. Cooperation & Dev., Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, O.E.C.D. Doc. C(80)58/FINAL (Sept. 23, 1980).

[5] *Id.*

order.[6] This remains the case, but in most states, data collectors can use, share, or sell the data they collect from an individual without telling them that they are doing so, or how they are using the data. Similarly, no national law regulates if or when a company must notify individuals if their data is subject to a breach or exposed to unauthorized parties.[7] However, since 2001, virtually all the most popular commercial websites have privacy notices. Under this regime, as long as companies give users notice and choice of their data practices, they are judged to be following the law.

The academic consensus is that given the size of the digital information economy and the reach of data markets and all forms of surveillance, this notice and choice regime leaves consumers with little protection. Not only do individuals rarely read privacy policies, which are often incomprehensible and full of legal jargon, but they also rarely have real choices.

There are, however, some important exceptions to the notice and choice regime. There are stricter rules that apply to particular sectors, in certain states, and that apply to the collection of data by the government. However, these rules are often also insufficient to meet the challenges of the digital age: Fourth Amendment protections don't extend to information gathered by the government by browsing or scraping the internet, as this is information that individuals have already given away. Similarly, sectoral rules are outdated — most were enacted in the 80s and the 90s. For example, health tech apps like 23AndMe are not covered by the rules that apply to traditional health care institutions. We will go over the basics of those rules and identify opportunities for builders to do better.

[6] Congress crafted a few industry-specific privacy statues, but left a large array of data collection and use unregulated. The Clinton Administration created the Information Infrastructure Task Force to explore the issue, which issued documents in 1995 and 1997 that largely recommended a self-regulatory approach.

[7] Thorin Kilowski, "The State of Consumer Data Privacy Laws in the U.S. (And Why It Matters)," *The New York Times*, September 6, 2021, https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

What are data markets and how do they work?

Traditional markets are based on property and contracts: a legal person has ownership of a good and transfers it to another party through a contract. The idea is that markets are a very efficient way to allow participants to find, and buy, what they are looking for. In data markets, data holders exchange data for profit. It is important to highlight that personal data markets are often criticized for enabling and strengthening corporate and government surveillance, but it is also important to remember that most data produced these days is not personal. Another critique is that data markets may also replicate or strengthen existing inequalities in the digital information economy. Further, just knowing what data is out there is hard (the information costs are high). Additionally, most data is currently collected by gatekeepers who are unwilling to trade it or exercise a lot of power in the terms of the exchange. These dynamics can be an issue for small businesses that would benefit from access to data to gain valuable insights.

One of the challenges of data markets is that the ownership regime of data remains unclear. Data is not a physical thing, so it can't be traditional property, and intellectual property does not grant protection to databases or individualized data, because facts cannot be copyrighted. Lawyers sometimes use privacy law or trade secret law to try to create forms of legally excluding others — like researchers or governments — from data, creating quasi-property rights over data. In practice, though, when data is being exchanged through markets, lawyers conceptualize data trading as trading *data rights*, and not the data itself. Trading parties sign contracts called Data Licensing Agreements (DLAs) and include a list of licensee rights (reprocessing rights, ownership of derived and usage data, etc.), a confidentiality notice establishing the confidentiality of data vis-a-vis third parties, and an explanation of the policies relating to the security of the data at stake.

Additional privacy rules that apply to specific sectors

Several sectors of the economy have so-called "sectoral privacy rules" that govern the collection, use, and disclosure of personal information by the key actors participating in them. If you are building something in any of these sectors, you should study them in depth — or, better, get some legal advice. Here's the general idea.

Protections to credit history: The Fair Credit Reporting Act (FCRA)[8] regulates how consumer reporting agencies can treat the information they collect. Consumer credit reporting agencies include credit bureaus, medical information companies, and tenant screening services. The FCRA limits who is allowed to see a credit report, what information the credit bureaus can collect, and how information is obtained.

Financial institutions: The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data.[9] Typical financial institutions are companies that offer consumers financial products or services like loans, financial or investment advice, or insurance.[10] Indeed, according to the law, only a company that is "significantly engaged" in financial activities is considered a financial institution. Key to its application, therefore, is the definition of whether a company is a financial institution, and some fintech companies are not covered. The act doesn't cover how information can be used by the financial institution itself.

Traditional health care institutions: The privacy rule of HIPAA — the Health Insurance Portability and Accountability Act — addresses the use and disclosure of individuals' health information, and their right to understand and control how it is used. A key goal is to ensure that health information is protected while allowing it to flow within the health system. Covered entities include health care providers and health plans, as well as the people working in these institutions, such as hospitals, pharmacies, and insurance companies. The law contains a list of permissible disclosure of information without individual authorization for treatment, payment, and (with certain limits) research and public health-related purposes.[11]

School records: The Family Educational Rights and Privacy Act (FERPA), gives parents and eligible students control of their educational records. It prevents educational institutions from disclosing "personally identifiable information in educational records" without written consent.

---

[8] 15 U.S.C. §§ 1681-1681x.

[9] More info: U. S. FTC, "How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act," Federal Trade Commission, https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.

[10] *Id.*

[11] U.S. Centers for Disease Control and Prevention, "Health Information & Privacy: FERPA and HIPAA," https://www.cdc.gov/phlp/publications/topic/healthinformationprivacy.html.

Email and other telecommunications providers: The Electronic Communications Privacy Act (ECPA)[12] restricts the real-time interception of a wire, oral, or electronic communication. A forbidden interception can be committed by using an electronic, mechanical, or other device (but not mere eavesdropping) and intentional access of a facility where electronic communication services are provided and obtained (such as emails that are not in transit). It also prohibits the installation of "pen registers" — devices that provide non-content information about the origin and destination of communications, such as the destination phone numbers.

Services for children: The Children's Online Privacy Protection Rule (COPPA) imposes certain limits on data collection for websites and companies that collect personal information from kids under 13. The rule makes it mandatory to post a privacy policy that clearly and comprehensively describes how and what data is collected, how it is used, and a description of parental rights (which include reviewing their child's information, directing companies to delete it, and refusing the collection). Parents must also be directly notified, and websites must get parental consent.[13]

Video or streaming: The Video Privacy Protection Act (VPPA) prevents the disclosure of VHS rental records. Courts have applied it to streaming services too, which basically means that they cannot share personal identifiable information, except for purposes provided in the law, to third parties.[14]

State privacy bills

In addition to the self-regulatory notice and choice regime and the sector-specific rules above, at least five states in the U.S. have introduced comprehensive privacy laws: California, Colorado, Connecticut, Virginia, and Utah. At the time of this writing, at least five more states are discussing privacy laws. You should keep an eye on those depending on where you plan to launch your service and product and where your clients or users will be. A good way to do so is via the International Association of Privacy Professional's U.S. State Privacy Legislation Tracker.

---

[12] This same type of limitation also applies to anybody who provides communication services over the internet (e.g., Verizon, AT&T, etc.). Put another way, these acts protect networked account holders' statutory privacy rights against third-party access to stored account information held by network service providers. It gets complicated fast, but basically, if the government wants to access any personal information — and remember, what *is* personal data is complicated, too — about you from a network service provider, then it needs a court order.

[13] U.S. Federal Trade Commission, "*Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*," https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business.

[14] Hulu Privacy Litigation, 2012 WL 3282960 (N.D. Cal. 2012).

Most state privacy laws are rather similar. They include provisions that give users a right to some type of notice, and create extra rights for users and obligations for the companies collecting data. With certain variance, consumers in these states typically have a right to:

- **Access** information has been collected about them and shared with third parties
- **Rectify** incorrect or outdated personal data about them
- **Request deletion** of personal data about them under certain conditions
- Request that their personal data be disclosed to them in a common file format, called **data portability**
- **Opt-out of sales** of their personal information to third parties

Fiduciary duties in the privacy law literature: are data holders like doctors or lawyers?

There is a movement in American privacy scholarship to view digital privacy in relational terms of trust and trustworthiness. Scholars in this strand have proposed creating a legal fiduciary or loyalty duty in information societies. These fiduciary duties would be like those that doctors and lawyers have to their patients and clients. According to the law, fiduciary obligations go beyond the ordinary obligation of good faith that applies to all commercial transactions. They are duties of care, confidentiality, and loyalty toward those being served in each context — medical patients, legal clients, children. Professor Jack Balkin, amongst other scholars, has suggested that "duties of confidentiality and care require digital companies to keep their customers' data confidential and secure."[15]

Most fiduciary duties are created by law because they often have important reach beyond the parties of the relationship. But there is an academic discussion on whether fiduciary duties could be created by contract. Builders, in any case, could thus adopt contracts that bind them to act like a fiduciary to their users, and commit themselves to act with confidentiality and the utmost care when processing their users' data.

[15] Jack Balkin, "The Fiduciary Model of Privacy," *Harvard Law Review*, Issue 134, Vol. 11 (2020), https://harvardlawreview.org/wp-content/uploads/2020/10/134-Harv.-L.-Rev.-F.-11.pdf.

Privacy laws in California, Colorado, Connecticut, and Virginia include a **right against automated decision-making**, which prohibits businesses from using an automated process as the sole way to make a decision about a consumer without any human input.

These laws also create additional obligations on businesses to:

- **Provide notice to consumers** about certain data practices, privacy operations, and privacy programs
- Treat consumers under a certain age — usually 13 or 16 — with an **opt-in default** for the sale of their personal information

With certain variance they also oblige companies to:

- **Conduct formal risk assessments** of privacy and/or security projects or procedures
- **Create a prohibition to discriminate** against consumers who exercise their privacy rights
- Comply with a **purpose limitation obligation** that prohibits the processing of personal information for purposes other than those for which it was collected

Government and law enforcement

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[16] In the context of data privacy, this has come to mean a "reasonable expectation of privacy" protects the people from a government search. If the government wants to look into your house, your papers or emails or text messages, or your effects (belongings), then it will need a warrant.

The reasonable expectation of privacy refers most immediately to a person in their home, but the case law has evolved to recognize that people take their reasonable expectation of privacy with them. They take it into phone booths, as in *Katz v. United States*, where the Supreme Court found that the defendant enjoyed a reasonable expectation of privacy while making private calls in a phone booth (and ruled that the FBI's warrantless tapping of the phone was illegal),[17] and they take it with them in their cars and geolocational movements, as in *United States v. Jones*, where the Court ruled that planting a GPS device on a suspect's car required a warrant.[18]

[16] U.S. Const. amend. IV.
[17] Katz v. United States, 389 U.S. 347 (1967).
[18] United States v. Jones, 565 U.S. 400 (2012).

A federal privacy law on the horizon?

At the time of writing this report, the U.S. Congress is discussing the American Data Protection and Privacy Act (ADPPA). As explained by Professors Neil Richards and Woodrow Hartzog, pioneers of the privacy as trust movement, this is "the most significant bipartisan privacy legislation introduced in more than a decade, and it represents an attempt to move beyond the ineffective notice and choice approach to privacy that has been the hallmark of U.S. legislators since the days of dial-up modems."[19]

Perhaps the most interesting provision of the bill is its duty of loyalty: Title I — "Duty of Loyalty." The section starts by creating requirements for data minimization, which require entities collecting data to limit the information they collect, process, and transfer to that which is "reasonably necessary, proportionate, and limited to" only what they need to provide or maintain specific products or services.[20] Professors Hartzog and Richards explain, however, that the bill falls short in this duty, even if strong data minimization rules are a key part of data loyalty. As they explain, "... data minimization is merely one aspect of acting in the best interests of trusting parties. Data loyalty rules should also cover manipulation, breaches of confidentiality, wrongful discrimination, and reckless and extractive engagement models. Data minimization rules only indirectly confront many of these issues."[21]

Nevertheless, there seems to be some convergence in Congress on data loyalty, as earlier bills and proposals were also anchored in duties of loyalty. Though the future of the bill remains unsure, it's a safe bet to prepare for a future where data processors have something similar to duties of loyalty toward users and data subjects.

More: https://iapp.org/news/a/were-so-close-to-getting-data-loyalty-right/

While this may seem reasonable and expansive, there is a catch: If a person voluntarily gives information to a third party, then the recipient can do whatever they want with that information, as can recipients going forward. This includes sharing it with the

[19] IAPP, "We're So Close to Getting Data Loyalty Right," accessed January 7, 2023, https://iapp.org/news/a/were-so-close-to-getting-data-loyalty-right/.
[20] *Id.*
[21] *Id.*

government. For instance, imagine that Jack and Jackie are penpals and that the government wants to read their letters on the suspicion that Jack smuggles and trades contraband. Government agents cannot read the letters in Jack's possession without a warrant, but they can read Jackie's letters if they ask Jackie and she lets them. This is called the third-party doctrine.[22] It's important to note that while the Electronic Communications Privacy Act does impose several limitations on the government's ability to collect information from a third party, it hardly prevents the government from using information that a third party voluntarily gives to the government.

One more important note on "privacy" itself: While these basics of Fourth Amendment jurisprudence focus on privacy as a kind of nondisclosure (protecting your data from the government's prying eyes), another kind of privacy courses through the Constitution, too. That is privacy as noninterference, the notion that people can make decisions about fundamental rights for themselves without any government interference (e.g., take contraception or marry whomever they please). The two are of course related, but distinguishable.[23]

Opportunities

As explained above, builders must be careful to comply with specific rules if their operations or product fall within one of the sectors that are specifically regulated or take place or have clients in one of the states with horizontal privacy laws. If this is not the case, however, there are few — if any — privacy protections that apply to builders in the U.S. (except whatever you are saying in your privacy policy, if you have one).

That does not mean there is little for builders to do. On the contrary, the self-regulatory approach invites builders to adopt good data governance practices in their operations. Through privacy policies and contractual arrangements, builders can create legal arrangements around data collection, processing practices, and operations that turn them into better data stewards in the digital information economy. [24]

In the sections that follow, we draw from the existing academic and policy literature on

---

[22] If the government wants bank records, it can compel the bank to hand them over (*United States v. Miller*). If the government wants phone records (the numbers dialed, when they dialed them, how long the calls lasted, etc.), it can compel the phone company to hand them over (*Smith v. Maryland*). If the government wants to know Jack's location, it can compel the phone company to hand over its cell site location data for Jack's phone for a seven-day period of time (*Carpenter v. United States*).

[23] Jeannie Suk Gersen, "Why the Privacy Wars Rage On," *The New Yorker*, June 27, 2022, https://www.newyorker.com/magazine/2022/06/27/why-the-privacy-wars-rage-on-amy-gajda-seek-and-hide-brian-hochman-the-listeners.

[24] A data steward is an intermediary body or person who manages data (rights) on behalf of beneficiaries within a consent-based structure and toward a defined goal.

ways to improve the digital information economy and adapt it to what builders could do with their own privacy policies. We dive deep into three opportunities: data collaboratives for risk management, data trusts for health data, and data commons for gig workers.

Before we go into our case studies, and if you want to keep it simple, the first thing builders could — and *should* do — is comply with the very basics of good and fair data governance principles that have been identified by documents like the Fair Information Practice Principles (FIPP) we briefly described above or other insights from other privacy rules. To do so, and in the interest of simplicity, we present a checklist for builders interested in adopting good, simple, data governance practices in their operations.

The basics of privacy notices and policies

By including the following elements in your privacy policies and making sure users consent to them through your privacy notices, you will advance the state of data protection in the U.S. It gets even better: the basics of good personal data governance are not difficult to understand, and it is easy to extrapolate from the brief explanation of the different privacy rules above.

Your privacy notices and policies should include the following:

- ☐ A commitment to only collect the data you need for the service you provide, no more
- ☐ A clear explanation of what data you collect, and why
- ☐ A commitment to not sharing (or selling!) personally identifiable data unless it's necessary to provide the service; if you are going to share or sell the data for any other reason, you should get explicit consent and authorization from your users and ensure data receivers will also uphold your users' rights
- ☐ A commitment to not discriminate against users who do not consent to nonessential uses of their data
- ☐ If you share data with business partners, a commitment to make sure your partners also commit to similar good data governance practices
- ☐ Names of the business partners, customers or brokers that have access to user data

- ☐ A commitment to delete personally identifiable data once you no longer need it to provide your service — this is both for your users' and the company's safety
- ☐ An avenue to grant users easy access to the data you have about them, and an easy and actionable way to correct it if inaccurate
- ☐ An avenue for users to ask you to delete data about them when it's no longer needed to provide the service
- ☐ A commitment to only share data with governmental authorities if they have a valid subpoena or warrant
- ☐ A commitment to delete and/or anonymize all data when you no longer need it
- ☐ An explanation, in a clear and succinct way, of all these rights and how and why you are using user data

Case Study #1: Data collaboratives for risk management

In this section:

- Data collaboratives, which are often organized as nonprofit organizations, can facilitate the sharing and pooling of data to unlock its collective value and serve public interest goals.
- They can be particularly helpful in sectors or areas where data is available but not shared, and where data sharing doesn't create competitive disadvantages, for example in risk management or sectors like public utilities.
- Access to data and insights derived from it is usually limited to those providing data to the collaborative to incentivize the supply of data.

What is it?

Data collaboratives are platforms that facilitate data exchanges for public interest goals.[25] The philosophy behind data collaboratives is that sharing data can generate public value in key areas such as risk and safety management,[26] prediction and forecasting,[27] and the design and improvement of public services.[28] They are seen as a potential solution to situations where data is available but is not pooled due to high transaction costs and lack of trusted intermediaries.[29]

Data collaboratives are typically nonprofit organizations that operate and run the data collaborative platform.[30] They have a clear mission, ranging from improving road safety to ameliorating disease prediction. They provide a platform for individuals, firms, and public bodies to share their own data in a trustworthy and safe manner in exchange for a service. The service can either take the form of data intelligence (e.g., insights on fire

[25] Data Collaboratives, accessed September 20, 2022, https://datacollaboratives.org/.
[26] Stefaan Verhulst and Andrew Young, "Battling Ebola in Sierra Leone: Data Sharing to Improve Crisis Response," *Open Data's Impact*, January 2016.
[27] International Centre for Climate Change and Development, "Mobile Data, Environmental Extremes and Population," accessed September 20, 2022, https://www.icccad.net/mdeep/
[28] California Data Collaborative, "Data and Analysis to Meet Big Water Efficiency Targets," accessed September 20, 2022, https://www.californiadatacollaborative.org/.
[29] Bram Klievink, Haiko van der Voort, and Wojnand Veeneman, "Creating Value Through Data Collaboratives," *Information Polity* 23 (December 2018): 379.
[30] Erna Ruijer, "Designing and Implementing Data Collaboratives: A Governance Perspective," *Government Information Quarterly* 38. no. 4 (October 2021): 101612.

risks for tourists)[31] or access to each other's data (e.g., research collaboratives that enable researchers to share their datasets).[32] To incentivize data supply, access to the data held by the collaborative or to the insights derived from the data is limited to the data providers.[33]

Data collaboratives are based on two principles: 1) voluntary data sharing by data producers/holders and 2) reaping the combinatorial benefits of data. The data shared can be personal, non-personal, or both. It ranges from personal disease records to traffic data collected by navigation apps. Whilst this data is already out there, in the absence of sharing incentives, it stays with the data producers and holders. Thus, a key contribution of data collaboratives is that they solve coordination problems by creating a trusted third party that holds and/or processes data. However, it is for the builders to identify the possible data suppliers and incentivize them to contribute. After a certain reputation is built, data suppliers may approach the data collaboratives directly, but in the beginning, it is for the collaboratives to create a community of data providers.

HiLo — sharing fleet data for maritime safety

An example of a data collaborative is HiLo, a nonprofit organization that invites shipping companies to provide monthly data about their fleet in exchange for both tailored and industry-wide analytics on risks and safety.[34] The goal of the platform is to "unlock the power of data to save lives." It pools data received from subscribing fleets, processes it using predictive analytics, and delivers individualized and collective insights based on the data provided. Instead of paying for the risk and safety analytics, fleet owners provide their data; this creates a circuit where the data of each fleet is used to enhance the safety of all participating fleets. Aligned with its public interest mission, HiLo exhibits good data security practices, as none of the individual fleet data is shared with any other participating fleets. The only information shared is in the form of high-level industry aggregates that do not mention the performance of any specific fleet.

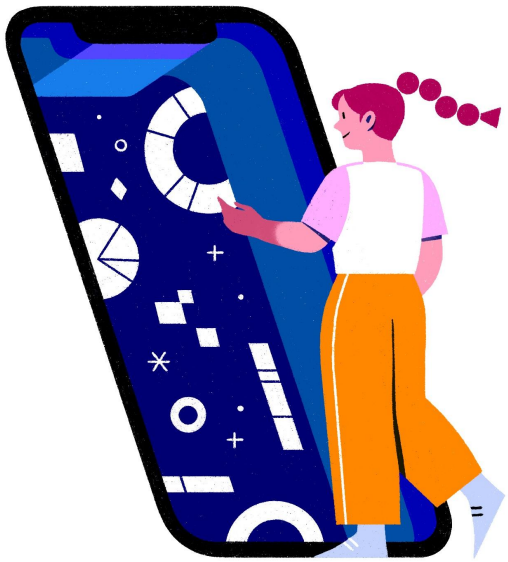
---

[31] Open Data Institute, "Case Study: The Value of Sharing Data for Benchmarking and Insights," accessed September 20, 2022, https://theodi.org/article/case-study-the-value-of-sharing-data-for-benchmarking-and-insights/.
[32] Data Collaboratives, "Eradicating Tuberculosis in India with the Help of Airtel Data," accessed September 20, 2022, https://datacollaboratives.org/cases/eradicating-tuberculosis-in-india-with-the-help-of-airtel-data.html.
[33] Bruno Carballa Smichowski et al., "Data-Driven Economy: Challenges and Opportunities," *Intereconomics* 54, no. 4 (2019): 200.
[34] HiLo, "What We Do," HiLo, accessed September 20, 2022, https://www.hilomrm.com/what-we-do/.

Building a data collaborative might be for you if...

Data collaboratives might be most useful in sectors or business functions where data is available, but is not shared due to high transaction costs, and data sharing might create value for many actors without creating threats for competition. This is the case for industries like public utilities and medical research or cross-sectoral business functions like risk and safety management. Data collaboratives address the problem of insufficient data resources and lower the costs of data gathering, thereby enabling innovation by small and medium market players who are routinely trapped in ecosystems where big players amass outsized datasets and restrict data access.[35] Data collaboratives can further reduce the transaction costs of data sharing, such as the cost of gathering information about potential sharing partners, and the cost of establishing a trustworthy infrastructure for exchanging data.

NetHope, for example, has gathered data from the private and the public sector in order to model the trajectory of the Ebola outbreaks in West Africa, hoping to materially contribute to the containment of the outbreak.[36] California Data Collaborative (CaDC) compiles data from California-based water utility agencies, providing an overview of how much, when, and where water is used with the ultimate goal of informing superior water management policies.[37]



The design of data collaboratives is centered around a data sharing protocol that specifies how the data is collected, aggregated, and processed (if applicable). Infrastructurally, this can take the form of a pigeonhole where data is manually updated, or of an API that enables the automatization of data sharing. Legally, this means that the data providers should be asked to sign a data licensing agreement that lays down the rights and obligations of both parties (more on this below).

---

[35] Alex Pentland, Alexander Lipton, and Thomas Hardjono, "Building the New Economy" (Cambridge: MIT Press, 2021), 1–15.

[36] Nethope, What We Do," NETHOPE, accessed September 20, 2022, https://nethope.org/.

[37] California Data Collaborative, Data Collaboratives, https://datacollaboratives.org/cases/california-data-collaborative-cadc-coalition-of-water-utilities.html.

Why do this? What are the potential benefits, limitations, and risks?

Data collaboratives are mechanisms to unlock the collective value of data. Their primary advantage is that they democratize access to data for stakeholders that would otherwise face difficulties, either because it is unavailable or too expensive. A further benefit of data collaboratives is that they do not only collect and aggregate data, but may also process it to generate insights that can lead to better policies, decisions, and design choices. Seen through this lens, collaboratives facilitate the production of knowledge.

A key limitation, however, is that the only data gathered is that of participants in the collaborative.[38] Consequently, if the player with key insights is, for example, a platform who is a predominant participant in the market and they do not want to join a collaborative, the collaborative might not really deliver on its promise. It is important, for collaboratives to work, that they are adopted in sectors where data is dispersed and not primarily controlled by one actor.

Given the fact that data collaboratives collect, aggregate, and process data that can be highly sensitive, they are exposed to several risks:

- **Private actors sharing data must be careful not to engage in cartel-like behavior.** If you are building a data collaborative that is open only to a few, it could look like you are behaving like a cartel in a market. Indeed, competition law prohibits competing firms from coordinating actions amongst themselves. Thus, sharing information on *the business* — instead of security or the weather — such as goods sold, prices, and future projects can form the basis of collusive behavior and might be risky.[39]
- **The data shared can be sensitive.** Developers need to make sure that the data is provided by parties that have the right to do so. Whilst tracing the pedigree of data may not be feasible, data exchanges *can* ask data providers to sign DLAs specifying that they had the right to transfer the data at stake. Similarly, it may be best not to share personal or sensitive information, but if it is shared, data collaboratives must ensure that the actor sharing the data has the explicit authorization to do so.
- **Pulling data together into one repository creates different forms of cybersecurity risks.** Make sure you adopt good architectures and risk models

[38] Andreas Rasche, Mette Morsing, and Erik Wetter, "Assessing the Legitimacy of Open and Closed Data Partnerships for Sustainable Development," *Business & Society* 60, no. 3 (February 2019): 547.
[39] Nicolo Zingales, "Data Collaboratives, Competition Law and the Governance of EU Data Spaces," in *Research Handbook on the Law and Economics of Competition,* ed. Ioannis Kokkoris and Claudia Lemus (Edward Elgar, 2022), 8–49.

that ensure the safety of your information. For the same reason, the less personal and sensitive information is involved, the safer the situation may be.

Where do you start?: The data collaborative checklist

- ☐ Ensure that the issue you are tackling is one where most actors would benefit from sharing information with each other.
- ☐ Identify the data you're talking about, the actors, and how the data should be used.
- ☐ Design a Data Licensing Agreement (DLA) that includes:
    1. A clause stating the data provider is either the producer of the data shared or has the right to share it with you
    2. The rights of different actors vis-à-vis the data shared: e.g. reprocessing rights, ownership of derived and usage data, etc.
    3. An explanation of the purposes for which the data is being processed and the types of metadata that is generated during processing

    It is recommended to also include policies that:

    1. Establish the confidentiality of the data vis-à-vis third parties and the extent to which the data is shared with the other data providers
    2. Specify who has control over the data once it is transferred (Can contributors delete it? Or once they transfer it, is it under the control of the collaborative?)
    3. Relate to the security of the data
- ☐ Design a reliable mechanism for data sharing. Some collaboratives require manual uploading on their websites, while others rely on APIs. The key is to minimize sharing costs while also ensuring adequate protection.

Additional resources

"Data Collaboratives Canvas," Observatory of Public Sector Innovation, https://oecd-opsi.org/toolkits/data-collaboratives-canvas/.

"Open Data Collaboratives," https://www.opendatacollaboratives.com/.

"Introduction to Data Collaboratives," Official Site of the State of New Jersey, https://skills.innovation.nj.gov/modules/data-collaboratives.html.

Iryna Susha, Marijin Janssen and Stefaan Verhulst, "Data Collaboratives as a New Frontier of Cross-Sector Partnerships in the Age of Open Data: Taxonomy Development," https://repository.tudelft.nl/islandora/object/uuid%3Aad261755-da4f-4da6-be1d-8180c53741f6.

Stefan Verhulst, Andrew Young and Prianka Srinivasan, "An Introduction to Data Collaboratives: Creating Public Value By Exchanging Data," https://datacollaboratives.org/introduction.html#learn-more.

Case Study #2: Trustworthy intermediaries for health data

In this section:

- Trustworthy intermediaries can help people exercise more control over their data if they are legally bound to manage said data in their interest.
- This approach is inspired by the concept of legal trusts, which create a legal arrangement in which a trustee manages a certain asset on behalf of a beneficiary to whom it owes a fiduciary duty.
- While it is still unclear to what degree this concept can be applied to data or rights over data, trustworthy (or trust-like) intermediaries can perform a similar function to advance people's interests in relation to their data, for example to protect their privacy in the health context.

What is it?

A data trust is a (potential) legal mechanism that has been proposed by scholars by which individuals could pool the rights over their data so that another person can manage those rights for their benefit.[40] The idea of establishing data trusts comes from the experience with trusts in other spaces, where one person (the settlor) places the rights associated with an asset in trust to be managed by another (the trustee), who holds and manages the rights associated with an asset for the benefit of a third (the beneficiary). Trusts are typically used when the rights holder has some difficulty managing their own rights (maybe a minor with a big inheritance or business partners who establish a trust to manage the funds of a joint venture), making it beneficial to have a third party managing the assets for them.

[40] Although there are a few pilot projects launching in the United Kingdom (a country with similar trust laws to the United States) and one community health project calling itself a data trust in the United States, data trusts exist mostly as proposed solutions to existing imperfect data governance regimes. *See, e.g.*, Data Trusts Initiative, https://datatrusts.uk/; Community Data Trust, Elevate Health, https://elevatehealth.org/solutions/community-data-trust; "Enabling Data Sharing for Social Benefit Through Data Trusts: Data Trusts in Climate," Global Partnership on Artificial Intelligence, March 2022, https://gpai.ai/projects/data-governance/data-trusts-in-climate-interim-report.pdf; Sylvie Delacroix & Neil Lawrence, "Bottom-up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance," 9 *International Data Privacy Law* 236, 2019, https://siliconflatirons.org/wp-content/uploads/2021/01/Bottom-Up-Data-Trusts-disturbing-the-one-size-fits-all-approach-to-data-governance.pdf.; Sean Martin McDonald, "Reclaiming Data Trusts," Centre for International Governance Innovation, March 5, 2019, https://www.cigionline.org/articles/reclaiming-data-trusts/.

A trust is a legal relationship, often explicitly allowed by a trust law. In the data governance space, data trusts have been proposed as alternatives to solve the problem of "privacy self-management" and information asymmetries, the problem individuals face when trying to understand the terms to which they agree when they consent to privacy notices, and more generally, when trying to exercise their privacy rights, such as whether they want to withdraw consent from a particular firm.[41] In the health tech space, for example, these kinds of structures allow individuals to contribute their personal and highly sensitive data for research purposes. A trustee, whose main job is to look after the interests of users or clinical study subjects, can give them some assurance of proper data handling. Similarly, since these structures are often set up to last for many years, this assurance can survive changes in personnel, projects, or company ownership.[42] Comparing these arrangements with other data sharing schemes, the particularity of data trusts is that an intermediary body is in charge of making the decisions about how the data is shared with others, and this intermediary has the particular duty to uphold the data rights holders' interests first. It may thus be particularly useful if the data you are pulling together is sensitive, or if you are dealing with vulnerable communities.

How does a trust work?

Trust law varies from state to state, but people can generally place almost any asset in trust, as long as they act with the clear intention to establish a trust, the asset to be placed in trust is clearly defined, and the beneficiary (or beneficiaries) are clearly defined. The trustee bears a fiduciary duty to act in the beneficiary's interest according to the terms of the trust, meaning that the trustee must not only follow the terms of the trust, but must also act with a duty of care, of loyalty, and of good faith (among other duties). If the trustee fails to live up to these duties, the beneficiaries can turn to the courts for remedy, which could include money damages or the removal of the trustee.

[41] "Bottom-up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance," 9 *International Data Privacy Law* 236 (2019), https://siliconflatirons.org/wp-content/uploads/2021/01/Bottom-Up-Data-Trusts-disturbing-the-one-size-fits-all-approach-to-data-governance.pdf.

[42] For a good example of a research project that has too many diverse interests and study subjects to adequately address the subjects' privacy concerns, see Joseph Goldstein, "Hospital and Drugmaker Move to Build Vast Database of New Yorkers' DNA," *The New York Times*, August 12, 2022, https://www.nytimes.com/2022/08/12/nyregion/database-new-yorkers-dna.html.

There is no law yet that explicitly allows for or creates data trusts. This section thus examines a few trusted intermediary bodies that act as we just described in the health data space. Because they act like trusts but legally actually aren't trusts, we call these "trustworthy intermediaries." When trusts or other fiduciary relationships are created by law there are strict legal requirements about how the assets and information held by the trust can be shared, especially with actors such as law enforcement. There is an academic and judicial debate on whether trusts can be established only by contract, but because the question is not settled, we will refer to the examples we present here as trustworthy intermediaries.

The Genomic Data Commons — an intermediary that facilitates cancer research

The Genomic Data Commons (GDC) is an initiative of the U.S. National Cancer Institute (NCI) to provide cancer researchers focusing on precision medicine with a repository and information base that enables data sharing across different cancer genomic studies. GDC was established to lead the NCI's effort in generating critical datasets for cancer research — supporting different large-scale programs, but also providing the research community at large the receipt, quality control, integration, storage, and redistribution of standardized cancer genomic datasets derived from various NCI programs.

Individuals who want to access the data must apply for permission from the National Center for Biotechnology Information (NCBI) Database of Genotypes and Phenotypes (dbGaP) and must also promise to not attempt to identify individual human research participants. Only senior investigators at a level equivalent to a tenure track professor and National Institutes of Health investigators can apply.[43] Similarly, dbGaP has a mandatory data management and sharing policy that establishes mechanisms and rules to keep data confidential and to limit its use to the research purposes approved by the intermediary.[44] These rules help address the highly sensitive nature of health, genomic, and phenotypic data. Consequently, while research participants consent to their data and samples collection and agree that it will be shared for research, GDC has an embedded mechanism where NIS acts like a trustworthy intermediary who ensures the rights and interests of patients, while contributing to the wider goal of making data available for research.

[43] U.S. National Cancer Institute, "GDC Policies," https://gdc.cancer.gov/about-gdc/gdc-policies.
[44] U.S. National Institutes of Health, "Using Genomic Data Responsibly," https://sharing.nih.gov/accessing-data/accessing-genomic-data/using-genomic-data-responsibly.

These all have functioning intermediaries that create a trust-like environment to improve the data management environment for users and builders. Thus, legal ambiguity shouldn't stop interested builders from setting up an intermediary and independent institution, with certain clear obligations and freedoms, whose main task is to guarantee the interests of the data subjects.

Building a trusted intermediary might be for you if...

If you work with data that warrants an intermediary to ensure the interests of data subjects, trustworthy intermediaries might be a good fit for you. This could be the case for very sensitive data. It may also be for builders trying to bring groups together and give them more control over their data by setting up rules about what gets shared, with whom, and under what conditions, and for builders who wouldn't mind appointing an independent actor to enforce said rules.

An example of an intermediary that gave users more control over their data was Data Does Good, a "consumer data collective" that "tried to help people pool together the value of their data" to provide a source of funding for charities.[45] They did so by setting up a browser extension that gathered anonymous information about the products people shopped for on Amazon, and then monetizing the insights of those shopping trends to fund the nonprofit organizations of their choice. At the same time, they had a separate tool called Loofa that continually monitored and scrubbed people's exposed personal information from the web. Data Does Good thus acted as a technical and institutional intermediary through which people could better assert and manage the interests they have over their data and shopping history by delegating some of that management to an intermediary. Through its interfaces, Data Does Good held and managed data and some of the insights associated with their shopping data and did so to benefit a party agreed to by data subjects. The project ran for two years before dissolving in 2018.

Why do this? What are the potential benefits, limitations, and risks?

Having a trusted and independent intermediary managing data promises two substantial improvements over some of the power imbalances present in the digital age. First, because data has almost no value unless in aggregate, individuals have almost no leverage in the modern data environment. Aggregating rights into a trust or a trust-like pool can give the manager of that pool the bargaining power inherent in aggregate data (importantly, this requires some technical form to collect the data at

[45] Crunchbase, "Data Does Good," Revised September 2022, https://www.crunchbase.com/organization/data-does-good.

source). Second, people delegating the management of some of their data rights to a trusted intermediary get to decide exactly what rights they are delegating and the conditions under which the trusted intermediary can exercise those rights. This gives people the power to specify what data they want out there, and what exactly "out there" means.

A hypothetical example: Reproductive health apps

Reproductive health apps, for example period tracking apps, are enormously popular in the United States; researchers estimate that about one third of women, transgender men, and nonbinary people who menstruate use them during some period in their lives.[46] But the vast majority, and certainly all of the most popular apps, have inadequate privacy protections for the user data they store on their servers and rely on to provide better products to their users.[47] Even if the app makers don't sell users' data to third parties, just storing user data on company servers could expose them to nefarious actors or — after the Supreme Court overturned *Roe v. Wade* — prosecution and bounty hunters. This issue is particularly pressing as period trackers are not covered by HIPAA, because they are considered lifestyle apps.

Consequently, if an app decided to create a trusted intermediary, or become itself a trusted intermediary (using the user's data only for the user's benefits, and for purposes specifically agreed to) some of this risk could be averted. The terms of the intermediation could limit what kind of data is collected and processed and dictate the conditions under which the company could access and use it. Because data trusts are not recognized by a law in the U.S., and it is still unclear whether they'd be recognized in court, it is likely that establishing such an arrangement would not insulate user data entirely from law enforcement. They could still access it with a judicial warrant. The terms of the trusted intermediation could, however, preclude the company from *selling* the data, which would in turn make it hard for malicious actors or governmental actors to access this sensitive information in the data market.

---

[46] Kaiser Family Foundation, "Health Apps and Information Survey," September 10, 2019, https://www.kff.org/other/poll-finding/kff-health-apps-and-information-survey/.

[47] Donna Rosato, "What Your Period Tracker App Knows About You," *Consumer Reports*, January 28, 2020, https://www.consumerreports.org/health-privacy/what-your-period-tracker-app-knows-about-you-a8701683935/.

Trusted intermediaries also offer organizations — companies, hospitals, governments, etc. — promising opportunities to set up trust-like relationships with the data subjects of information they would like to process for legitimate interests. A company would sponsor the creation of a data trust, for instance, to realize its commitment to customer privacy, while simultaneously having a third party make sure that the data processing is done in a fair and responsible way.

As we said earlier, though, data trusts mostly exist in legal academic literature. One reason may be that they pose a set of important challenges that builders trying to set up trusted intermediaries may also encounter. First, articulating the data rights to be conferred to the intermediary entity and, second, ensuring the intermediary has actual control over the data. Indeed, the idea of data trusts stems from concerns over how personal data is being monetized online and whether and how that can hurt individuals and societies by, for example, manipulating different forms of choice or inciting polarization. It is unclear, however, how these bodies could work without the agreement of big tech platforms. Social media platforms, for example, are the ones that produce data about users' browsing history and then immediately store it in their servers for analysis. It is difficult to know, in this example, when and where an independently built data trust could intervene.

There are other instances, however, where data sharing is less ubiquitous, must be explicitly shared by individuals, and where the actors involved have a clear interest in ensuring users trust how their data is being processed and used. Here they may have great potential. The Genomic Data Commons, presented above, is of this kind.

It may well be that in instances where data is sensitive and unprotected, having a trusted intermediary manage that data could accomplish important things to isolate data subjects' interests from any eventual commercial interests and could keep users' personal health data safer than it is now. This would happen by virtue of having a trusted and neutral intermediary through mandatory bylaws and data governance policies that determine what — and under what condition — data can be used and shared, and whose main job it is to look out for users.

Where do you start? The data trust or trusted intermediary checklist

- ☐ Start by asking yourself if you are addressing a problem where one person can work on behalf of a group of people to protect their privacy or their interests over their data, and whether it is possible to guarantee access and control over that data.
- ☐ Identify the key actors of the relationship you are building:

- ☐ Who would be the settlors — the person(s) putting data into trust or the trusted intermediary? This will most likely be the person(s) whose data interests you are interested in safeguarding.
- ☐ Who would be the beneficiary? Are they the person for whose benefit the trust exists (for example, medical researchers)? In some cases, the settlor and the beneficiary could be the same person, as in the case of some health tracking applications.
- ☐ Who would be the trustee or trusted intermediary (the person responsible for administering the trust)?

☐ Identify the data rights and/or interests you want to protect and how. For example, the kind of parties or organizations with whom you would be comfortable sharing said data rights, and the uses you'd be comfortable with. You could, as a builder, set up a decision-making mechanism for the settlors to decide.

Then follow one of the following two paths:

PATH 1: If you want to try to set up a trust:

☐ Hire a trust and estates lawyer and a privacy lawyer.

☐ Get your lawyers to draft a trust document that comports with your state's laws that articulates (1) a clear intent to create a trust, (2) the asset to be placed in trust, and (3) the beneficiaries of the trust.

☐ Build a technical infrastructure — like an API or platform — that allows you to "place" the data in the hands of the trustee and make it accessible to the beneficiary, while being under the control and audit of the trustee. In most consumer scenarios you would need a plug-in of some sorts. Note that a difficulty in this model is that not all users have easy access to their own data.

☐ Articulate how you want a trustee to act on the beneficiary's behalf. What's their role and how do they do it?

PATH 2: Build a trusted intermediary that will be in charge of upholding user's interest:

☐ Identify the data you want to be managed by the intermediary, and how you are going to pool it.

☐ Build the platform or sharing/pooling mechanism.

- ☐ Write a data management policy that establishes how data will be accessed, or how data will be further shared by your intermediary.
- ☐ Make the policy binding by directly referencing it in your privacy notice (to be accepted by data subjects) and in a contract with the intermediary party you selected. Establishing these policies in some sort of legal document, or making them binding through a legal document, will give data subjects more protection.
- ☐ Decide on an intermediary person or body within or outside your institution who will enforce the data policy. Legal agreements that guarantee independence and choosing an NGO, a university, or another somewhat separated body will ensure there is more independence. (They will also be bound by contract to be independent and act on behalf of users' best interest.)

Additional resources

Ada Lovelace Institute, "Exploring legal mechanisms for data stewardship," March 4, 2021, https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/.

Element AI and Nesta, "Data Trusts: A new tool for data governance," 2019, https://hello.elementai.com/rs/024-OAQ-547/images/Data_Trusts_EN_201914.pdf.

Richard Milne, Annie Sorbie, & Mary Dixon-Woods, "What Can Data Trusts for Health Research Learn from Participatory Governance in Biobanks?" 48 *Journal of Medical Ethics* 323 (2022), https://jme.bmj.com/content/medethics/48/5/323.full.pdf.

Sean Martin McDonald, "Reclaiming Data Trusts," Centre for International Governance Innovation (March 5, 2019), https://www.cigionline.org/articles/reclaiming-data-trusts/.

Sylvie Delacroix and Neil D. Lawrence, "Bottom-up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance," 9 *International Data Privacy Law* 236 (2019), https://siliconflatirons.org/wp-content/uploads/2021/01/Bottom-Up-Data-Trusts-disturbing-the-one-size-fits-all-approach-to-data-governance.pdf.

Case Study #3: Data co-ops and the platform economy

In this section:

- Inspired by the idea of cooperatives (or co-ops), data co-ops are collectively owned and democratically governed associations that manage and leverage data collected from their members (and potentially others).
- Setting up a data co-op requires the necessary data infrastructure and effective democratic governance rules and structures.
- In the labor context, data co-ops could be used to crowdsource workers' data and use it to improve their bargaining position vis-à-vis employers or online labor platforms.

What is it?

A cooperative (or co-op), in general, is an association of persons who gather to meet a common economic or social goal through a collectively owned and democratically controlled entity. A data cooperative is such an entity; it's a legal construct that facilitates the collaborative pooling of data by individuals or organizations for the economic, social, or cultural benefit of the group. In data co-ops, the legal entity usually administers some sort of software and interface — an app or website, for example — that gives insights or manages the data in the ways defined by the entity.

Worldwide, there are a few data cooperatives that pull data from the participants and, in doing so, try to solve for their members some of the issues often associated with the platform economy. These range from personal concerns — like privacy or labor rights — to societal and economic concerns — like who gets to benefit from the insights that pooled data delivers. Data cooperatives are collectively governed, and they seek to benefit each member individually, and empower all members as a collective.

Building a data co-op might be for you if...

Data cooperatives may be particularly relevant for sectors where information asymmetries play a significant role in creating a problem. This is the case for students in surveilled and remote educational environments, all sorts of gig workers, and workers in widely digitized warehouses, who could use better insights into the data they are co-producing on these platforms to improve their bargaining position. At least theoretically, even small and medium enterprises (SMEs) that rely on platforms' digital

marketplaces to sell their products could be members of a co-op (but participating in a co-op may be against their bylaws, so SMEs could be better off establishing a data collaborative as discussed in Case Study #1).

Driver's Seat — A data cooperative to empower gig workers through transparency

Driver's Seat is a cooperative of on-demand drivers who gather their own combined driving data in an app to help them have more leverage and gain insights that are usually kept secret by employers. Indeed, since the early days of the gig economy, professional drivers have found ways around some of these new forms of control by sharing information on pricing for individual rides, salary disparities, and other information in online driver forums and WhatsApp groups.[48] Since drivers often work alone, these forums are also very useful and primarily used to communicate routine workplace matters, like what to do in unsafe situations.[49]

Driver's Seat is a parallel app that collects data from drivers and analyzes it to help them understand their performance and earn more. Users can enable automatic tracking, which connects the platform to the rideshare and delivery platforms they use for work and automatically imports their gig activities and earnings into Driver's Seat. The option to log data manually also exists. Additionally, the app accesses workers' location to track their mileage.

Driver's Seat's business model is around selling data. To provide free data insights and services to gig workers, they pool and sell shared data to customers who support and understand their "driver first" mission. Clients include cities and transportation agencies that use the pooled data to understand work and transportation issues in the city.

Driver's Seat is a cooperative owned by rideshare and delivery drivers. Its members elect and serve on the co-op's board and are eligible for a share of its profits. From the information that is available, it doesn't seem like all users are members of the co-op, but all members and users are ride-hailing or delivery drivers.

[48] Alex Rosenblat, "The Network Uber Drivers Built," *Fast Company*, January 9, 2018, https://www.fastcompany.com/40501439/the-network-uber-drivers-built.
[49] *Id.*

The gig economy is an industry where data cooperatives may have important potential because it's very data-intensive and data is used by companies to run experiments and improve their gains at the margin, often in ways that are hard for workers to understand.[50] Indeed, one of the main challenges for individuals working in the platform economy is their further disempowerment vis-à-vis algorithmic management, digital surveillance in the workplace (whether in an office or a car), the gamification of work, and lack of control and information about when their work contracts might be terminated.

Antonio Aloisi and Valerio De Stefano, in *Your Boss is an Algorithm*, and Alex Rosenblat, in *Uberland: How Algorithms Are Rewriting the Rules of Work*, have identified that companies increasingly track a variety of personal and personalized statistics — such as ride acceptance rates, cancellation rates, and hours spent logged into the app — and then display them selectively to individual drivers to nudge them into actions. Similarly, through policies like surge pricing and rating systems, companies have further control over driver' income and contracts. There is little accountability and transparency about how algorithms — and the companies behind them — make decisions, which disempowers workers.

Data co-ops thus offer a valuable remedy for participants in the platform economy who could benefit from understanding how decisions are made — insights that can be derived from collective data-pooling.

Why do this? What are the potential benefits, limitations, and risks?

Data co-ops can offer members and users the service of pooling information, analyzing it, and delivering it back synthesized — something that is hard to do in many online forums. A co-op can also participate in the marketplace for data on behalf of its members (as in the case of Driver's Seat), upholding its mission and increasing the community of beneficiaries' bargaining power and the value of their aggregated data.

Despite their advantages, it is important to keep in mind co-ops' limitations and risks. A key limitation is that data co-ops will likely not solve the systemic or labor issues at play. They have the potential to give users and members some tools to derive value from their collective data and increase their leverage and bargaining power in their current situation, but not necessarily to tackle those situations themselves. As for the risks, it is important to keep in mind that collective governance and ownership is not

[50] Noam Scheiber, "How Uber Uses Psychological Tricks to Push Its Drivers' Buttons," *The New York Times*, April 2, 2017, https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html.

equivalent to good governance. While it is true that collective governance may lead to a better representation of stakeholders' interests, groups and leadership should also be treated carefully. To avoid problems downstream, it is important to have clear governance covenants that set out the mission of the co-op, clear limits on what can be done with the pooled data, and clear procedures about how decisions are made to ensure due process.

A different co-op: Grower Information Services Cooperative

Grower Information Services Cooperative (GiSC) is a farmer-owned data cooperative in Lubbock, Texas. Its mission is to help members navigate the fast-growing world of ag-tech by helping them collect, store, manage, and leverage their agricultural data. GiSC has partnered with IBM and MainStreet Data and offers member producers access to weather data and a data analytics platform called AgHub that collects and stores producers' data and aggregates it with other members' data to benchmark it and inform better farming decisions.

GiSC collects irrigation, agronomic, land, farm management, machine, and weather data. According to its data use agreement, members own the agricultural data that originates from their own farm, devices, and equipment, and members have a right to share, download, and delete their data at any moment. Members transfer data to GiSC through a limited license to use their data to provide the services above, and must specifically consent to their data being aggregated to the data pool of all members. Exceptionally, GiSC shares data with third parties outside the co-op, but it asks for prior consent from members before doing so. Third parties may include government or trusted advisors, or organizations facilitating technical integrations.

GiSC is a not-for-profit corporation owned by its members. To be a member, members must be engaged in the production of agricultural products and submit an application. Members can be natural persons or corporations. The board of directors, or a body authorized by them, accepts new members. Membership is $50 USD a month, and it grants access to GiSC services and voting powers. The co-op is governed by the board, which is selected by members. The co-op's bylaws rule its governance, including provisions for yearly meetings, requirements of quorum to make decisions, and how to elect the board.

Where do you start?

Start by clearly identifying your problem and community. Remember that data co-ops are particularly beneficial to address issues where information asymmetries exist. Further, you should get legal advice and explore extensive resources like Co-opLaw.org to set up the cooperative, its governance structure, and its data governance rules. In general, though, the checklist below outlines the main steps you should take.

The data co-op checklist

- ☐ **Diagnose your problem.** Is the problem you want to solve one that can be at least partially addressed by giving members of a group access to each other's data and insights derived from it?
- ☐ **Identify the community.** Is there a defined group of stakeholders, with similar interests and goals, who share that problem and could participate in the co-op? (Note: "farmers," "ride-hailing drivers," and "doctors and patients" are better defined and have more common interests than say, "consumers" or "citizens.")
- ☐ **Identify the data you need.** What data do you need to crowdsource from members to solve the problem?
- ☐ **Decide on delivery.** Identify the best way to deliver insights to your members.
- ☐ **Set up your co-op governance structure and rules.** You need to have:
    - The principles and goals of your data co-op
    - A clear definition of who can be a member and what they need to contribute to be one
    - A breakdown of who makes what decisions, a process to pick them, and how those decisions are made (including board election, frequency of meetings, delegates, quorum, etc.)
    - For large co-ops, an explanation of other roles you might want to have within the organization to advance executive tasks, such as a president, a financial officer, or — for our purposes — a data officer
    - Your business model
- ☐ **Set up a data management policy.** The policy should (at least) answer these questions:

- What data do you need?
- How will data be processed?
- Who within the co-op will have access to the data?
- Whom else will the data be shared with, and how?
- How and when can members retrieve their data?
- When will data be deleted?

Additional resources

Alex Pentland et. al, “Data Cooperatives: Digital Empowerment of Citizens and Workers,” MIT Connection Sciences, 2019, https://ide.mit.edu/wp-content/uploads/2019/02/Data-Cooperatives-final.pdf?x96981.

Co-opLaw, Co-opLaw.org.

Elettra Bietti et, al., “Data Cooperatives in Europe: A Legal and Empirical Investigation,” Berkman Klein Center (White Paper), December 2021, https://cyber.harvard.edu/sites/default/files/2022-02/Data_Cooperatives_Europe-group2.pdf.

Ernst Hafen, “Personal Data Cooperatives — A New Data Governance Framework for Data Donations and Precision Health,” The Ethics of Medical Data Donation, edited by Jenny Krutzinna et. al., Springer, 16 January 2019. pp. 141–149. doi: 10.1007/978-3-030-04363-6_9.

Platform Cooperativism Consortium, Platform.coop.

Trebor Scholz, “Uberworked and Underpaid: How Workers Are Disrupting the Digital Economy,” 1 edition. Cambridge, UK; Malden, MA: Polity, 2016. pp. 155-192.

Glossary

Builders: Builder is a term used in the alternative data governance sphere to refer to those entities — companies or individuals — who are devising new initiatives that employ models of alternative data governance.

Data Collaborative: Data collaboratives are third party-managed platforms (often nonprofit organizations) that facilitate data exchanges between participants (often companies) from different sectors for a set public interest goal. An illustrative example is that of the California Data Collaborative, whose platform compiles data from California-based water utility agencies to better understand the how, when, and where of water usage with the goal of better informing water management policies in the state. Data collaboratives can be a type of data steward.

Data collaboratives are based on the principles of voluntary data sharing and the reaping of collective benefits from data. Access to data held by the collaborative is often limited to the data providers. After a reputation is constructed, data suppliers may start to directly approach the data collaborative. However, in the development stages of collaboratives, it often falls upon them to ensure a steady community of data providers is created. It is important for new builders to acknowledge that collaboratives do carry certain risks.

Data Cooperative: A data cooperative is a collectively owned and democratically controlled legal entity that facilitates the collaborative pooling of data by individuals or organizations for the economic, social, or cultural benefit of the group. In data co-ops, the legal entity usually administers some sort of software and interface — an app or website, for example — that gives insights or manages the data in the ways defined by the entity.

Data Governance: According to the Data Futures Lab Glossary, data governance "describes who has power to make decisions over data and how."[51] The term has to do with the rules and structures that govern how data is collected, controlled, accessed, and shared.

Data Steward: A data steward is an intermediary body that manages data rights on behalf of beneficiaries within a "consent based structure and towards a defined goal."[52]

---

[51] Mozilla Foundation, "Data Futures Lab Glossary," accessed January 9, 2023, https://foundation.mozilla.org/de/data-futures-lab/data-for-empowerment/data-futures-lab-glossary/#data-governance.

[52] Mozilla Foundation, "Data Futures Lab Glossary," accessed January 9, 2023, https://foundation.mozilla.org/de/data-futures-lab/data-for-empowerment/data-futures-lab-glossary/#data-governance.

A data steward often relies on a legal structure that can be contractual, participatory, or based on a fiduciary relationship.[53]

Data Trust: A data trust is a proposed legal mechanism devised by scholars that would allow individuals to pool their data rights together and entrust it to another person (a third party) who would manage those rights on their behalf. The trustee (or settlor) would bear fiduciary duty to act in the set beneficiary's best interest according to the terms of the trust agreement. A trust is a legal relationship, often explicitly allowed by a trust law. However, in the data governance sphere, data trusts are yet to be formally created or allowed by law, and thus in practice they diverge in the protections granted to trusts in other industries, and still mostly exist only in legal academic literature.

Fiduciary Duty: A fiduciary duty is a type of legal obligation that goes beyond the standard good faith required of all commercial transactions. Fiduciary duties mean duty of care, confidentiality, and loyalty toward those they have been entrusted to serve. The standard of care within alternative data governance would be similar to those expected of doctors toward their patients or lawyers toward their legal clients.

Fourth Amendment: The Fourth Amendment of the U.S. Constitution protects people from unreasonable searches and seizures by the government, and requires that warrants are issued, upon probable cause.[54] This means that the government can only access personal information, or someone's property, with a warrant. The Fourth Amendment doctrine has relaxed over the years, however, to require a lower threshold for administrative inspections (such as restaurant health inspections).

Worthy of attention for the purposes of this report is that, according to the Third Party Doctrine, the protections of The Fourth Amendment do not extend to information that has voluntarily been revealed or shared by its subject to a third party. In 2018, however, the Supreme Court carved out a narrow exception to the third party doctrine. In *Carpenter v. United States*,[55] the Court held that the government violated the Fourth Amendment to the Constitution when it accessed historical cell site location information records containing the physical locations of someone's cell phone for many months without a search warrant.

---

[53] Mozilla Foundation, "Data Futures Lab Glossary," accessed January 9, 2023, https://foundation.mozilla.org/de/data-futures-lab/data-for-empowerment/data-futures-lab-glossary/#data-governance.

[54] United States Courts, "What Does the Fourth Amendment Mean?" accessed January 9, 2023, https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0.

[55] 138 S.Ct. 2206 (2018).

Personal Data (Personal Information): Personal data typically is information that can allow for the identity of its bearer to be revealed. Importantly, personal data is a legal definition that leads to higher standards of data protection. Because it is a legal definition, different legal regimes may have slightly different definitions: The GDPR, for example, defines personal data as "any information relating to an identified or identifiable natural person ('data subject')." The California Consumer Privacy Act talks about "personal information," which it defines as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." According to the U.S. Department of Labor, personal data, or "personal identifiable information," can be defined as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means."[56] Eventually, different definitions may lead to different standards of protection.

Platform Economy: Platform economy is used to describe the increasing movement of businesses from traditional to digital business models centered around platforms, resulting in the emergence of a new digitally based economy centered on platform services. Platform, in this sense, is an ambiguous term used to describe a significant part of the digital information economy. Platforms are data-driven companies and apps and websites like Uber, Facebook, and Airbnb that operate two-sided marketplaces, often granting one side of the transaction to user-generated content or services. Many of the companies operating these services also refer to themselves as platforms.[57]

[56] U.S. Department of Labor, "Guidance on the Protection of Personal Identifiable Information," accessed January 9, 2023, https://www.dol.gov/general/ppii#:~:text=Personal%20Identifiable%20Information%20(PII)%20is,either%20direct%20or%20indirect%20means.

[57] Martin Kenney and John Zysman, "The Rise of the Platform Economy," *Issues in Science and Technology* (blog), April 1, 2016, https://issues.org/rise-platform-economy-big-data-work/.

Bibliography

Ada Lovelace Institute. “Exploring Legal Mechanisms for Data Stewardship.” March 4, 2022. https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/.

Balkin, J. “The Fiduciary Model of Privacy.” *Harvard Law Review*, Issue 134, Vol. 11 (2020). https://harvardlawreview.org/wp-content/uploads/2020/10/134-Harv.-L.-Rev.-F.-11.pdf.

Bietti, E., A. Etxeberria, M. Mannan and J. Wong.. “Data Cooperatives in Europe: A Legal and Empirical Investigation.” Berkman Klein Center (White Paper). December 2021. https://cyber.harvard.edu/sites/default/files/2022-02/Data_Cooperatives_Europe-group2.pdf.

Botero Arcila, B. “The Case for Local Data Sharing Ordinances.” *William & Mary Bill of Rights Journal* (Forthcoming).

California Data Collaborative. “Data and Analysis to Meet Big Water Efficiency Targets.” Accessed September 20, 2022. https://www.californiadatacollaborative.org/.

California Data Collaborative. Data Collaboratives. https://datacollaboratives.org/cases/california-data-collaborative-cadc-coalition-of-water-utilities.html.

Co-opLaw. http://www.co-oplaw.org.

Crunchbase. “Data Does Good.” Revised September 2022. https://www.crunchbase.com/organization/data-does-good.

Data Collaboratives. Accessed September 20, 2022. https://datacollaboratives.org/.

Data Collaboratives. “Eradicating Tuberculosis in India with the Help of Airtel Data.” Accessed September 20, 2022. https://datacollaboratives.org/cases/eradicating-tuberculosis-in-india-with-the-help-of-airtel-data.html.

Data Trusts Initiative. https://datatrusts.uk/.

Delacroix, S. & N. Lawrence. “Bottom-up data Trusts: Disturbing the ‘One Size Fits All’ Approach to Data Governance.” 9 *Int’l Data Privacy Law* 236 (2019). https://academic.oup.com/idpl/article/9/4/236/5579842.

Determann, L. “No one Owns Data.” *Hastings Law Journal* Vol. 70, Issue 1, 1-44.

Element AI & Nesta, “Data Trusts: A New Tool for Data Governance.” 2019. https://hello.elementai.com/rs/024-OAQ-547/images/Data_Trusts_EN_201914.pdf.

Elevate Health Community Data Trust. https://elevatehealth.org/solutions/community-data-trust.

Global Partnership on AI. “Enabling Data Sharing for Social Benefit Through Data Trusts: Data Trusts in Climate.” March 2022. https://gpai.ai/projects/data-governance/data-trusts-in-climate-interim-report.pdf.

Goldstein, J. “Hospital and Drugmaker Move to Build Vast Database of New Yorkers’ DNA.” *The New York Times*, August 12, 2022. https://www.nytimes.com/2022/08/12/nyregion/database-new-yorkers-dna.html.

The GovLab. Data Collaboratives. https://datacollaboratives.org/.

Hafen, Ernst. “Personal Data Cooperatives – A New Data Governance Framework for Data Donations and Precision Health.” *The Ethics of Medical Data Donation*, edited by Jenny Krutzinna et. al., Springer, January 16, 2019. pp. 141–149. doi: 10.1007/978-3-030-04363-6_9.

Health Data Collaborative, “What We Do,” https://www.healthdatacollaborative.org/what-we-do/.

HiLo, “What We Do,” HiLo, accessed September 20, 2022, https://www.hilomrm.com/what-we-do/.

Hulu Privacy Litigation, 2012 WL 3282960 (N.D. Cal. 2012).

IAPP. “We’re So Close to Getting Data Loyalty Right.” Accessed January 7, 2023. https://iapp.org/news/a/were-so-close-to-getting-data-loyalty-right/.

International Centre for Climate Change and Development. “Mobile Data, Environmental Extremes and Population.” Accessed September 20, 2022, https://www.icccad.net/mdeep/.

Kaiser Family Foundation. “Health Apps and Information Survey.” September 10, 2019. https://www.kff.org/other/poll-finding/kff-health-apps-and-information-survey/.

Kapzcinsky, A. “The Law of Information Capitalism.” *The Yale Law Journal* Vol. 129, 1460.

Katz v. United States, 389 U.S. 347 (1967).

Kenney, M. and J Zysman. “The Rise of the Platform Economy.” *Issues in Science and Technology* (blog), April 1, 2016. https://issues.org/rise-platform-economy-big-data-work/.

Kilowski, T. “The State of Consumer Data Privacy Laws in the U.S. (And Why It Matters),” *The New York Times*, September 6, 2021. Available at: https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

Klievink, B., H. van der Voort and W. Veeneman. “Creating Value Through Data Collaboratives.” *Information Polity* 23 (December 2018): 379.

McDonald, S. “Reclaiming Data Trusts.” Centre for International Governance Innovation. March 5, 2019. https://www.cigionline.org/articles/reclaiming-data-trusts/.

McFarlane, B.. “Data Trusts and Defining Property,” *Oxford Faculty of Law Blogs,* October 29, 2019. https://blogs.law.ox.ac.uk/research-and-subject-groups/property-law/blog/2019/10/data-trusts-and-defining-property.

Milne, R. et. al. “What Can Data Trusts for Health Research Learn from Participatory Governance in Biobanks?” 48 *Journal of Medical Ethics* 323 (2022), https://jme.bmj.com/content/medethics/48/5/323.full.pdf.

Ministerial Council of the Org. for Econ. Cooperation & Dev., Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, O.E.C.D. Doc. C(80)58/FINAL (September 23, 1980).

Mozilla Foundation. ‘‘Data Futures Lab Glossary.” Accessed January 9, 2023. https://foundation.mozilla.org/de/data-futures-lab/data-for-empowerment/data-futures-lab-glossary/#data-governance.

Nethope. “What We Do.” NETHOPE. Accessed September 20, 2022. https://nethope.org/.

New Jersey. “Introduction to Data Collaboratives,” Official Site of the State of New Jersey. https://skills.innovation.nj.gov/modules/data-collaboratives.html.

Open Data Collaboratives. https://www.opendatacollaboratives.com/.

Open Data Institute. “Case Study: The Value of Sharing Data for Benchmarking and Insights.” Accessed September 20, 2022. https://theodi.org/article/case-study-the-value-of-sharing-data-for-benchmarking-and-insights/.

Pentland, A., A. Lipton and T. Hardjono. “Building the New Economy.” (Cambridge: MIT Press, 2021), 1–15.

Pentland, A., T. Hardjono, J. Penn, C. Colclough and L. Mandel. “Data Cooperatives: Digital Empowerment of Citizens and Workers.” *MIT Connection Sciences*, 2019. https://ide.mit.edu/wp-content/uploads/2019/02/Data-Cooperatives-final.pdf?x96981.

Pistor, K. “Rule by Data: The End of Markets?” *Law and Contemporary Problems* 83, no.2 (2020): 101.

Platform Cooperativism Consortium. platform.coop.

Rasche, A., M. Morsing and E. Wetter. “Assessing the Legitimacy of Open and Closed Data Partnerships for Sustainable Development,” *Business & Society* 60, no. 3 (February 2019): 547.

Richards, N. *Why Privacy Matters*, Oxford University Press (2022).

Rosato, D. “What Your Period Tracker App Knows About You.” *Consumer Reports*, January 28, 2020. https://www.consumerreports.org/health-privacy/what-your-period-tracker-app-knows-about-you-a8701683935/.

Rosenblat, A.. “The Network Uber Drivers Built.” *Fast Company*, January 9, 2018. https://www.fastcompany.com/40501439/the-network-uber-drivers-built.

Ruijer, E. “Designing and Implementing Data Collaboratives: A Governance Perspective.” *Government Information Quarterly* 38. no. 4 (October 2021): 101612.

Scheiber, N. “How Uber Uses Psychological Tricks to Push Its Drivers’ Buttons.” *The New York Times*, April 2, 2017. Available https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html.

Scholz, T. *Uberworked and Underpaid: How Workers Are Disrupting the Digital Economy.* 1 edition. Cambridge, UK; Malden, MA: Polity, 2016. pp. 155-192.

Smichowski, B. C., B. Engels, J. Haucap, C. Olk, M. Spiekermann, M. von Grafenstein and A. Wernick. “Data-Driven Economy: Challenges and Opportunities.” *Intereconomics* 54, no. 4 (2019): 200.

Solove, D. J. and W. Hartzog. “The FTC and the New Common Law of Privacy” (August 15, 2013). 114 Columbia Law Review 583 (2014), GWU Legal Studies Research Paper No. 2013-120, GWU Law School Public Law Research Paper No. 2013-120, Available at SSRN: https://ssrn.com/abstract=2312913 or http://dx.doi.org/10.2139/ssrn.2312913.

Suk Gersen, J. “Why the Privacy Wars Rage On.” *The New Yorker*, June 27, 2022. https://www.newyorker.com/magazine/2022/06/27/why-the-privacy-wars-rage-on-amy-gajda-seek-and-hide-brian-hochman-the-listeners.

United States Courts. “What Does the Fourth Amendment Mean?” Accessed January 9, 2023. https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0.

United States v. Jones, 565 U.S. 400 (2012).

U.S. Centers for Disease Control and Prevention. “Health Information & Privacy: FERPA and HIPAA.” https://www.cdc.gov/phlp/publications/topic/healthinformationprivacy.html.

U.S. Const. amend. IV.

U.S. Department of Health, Education and Welfare. “Records, Computers, and the Rights of Citizens: Report of the Secretary’s Advisory Committee on Automated Personal Data Systems.” 41–42. 1973. https://epic.org/documents/hew1973report/.

U.S. Department of Labor, “Guidance on the Protection of Personal Identifiable Information.” Accessed January 9, 2023. https://www.dol.gov/general/ppii#:~:text=Personal%20Identifiable%20Information%20(PII)%20is,either%20direct%20or%20indirect%20means.

U.S. Federal Trade Commission. “Children’s Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business.” https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business.

U.S. Federal Trade Commission. “How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act.” https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.

U. S. Federal Trade Commission Act of 1914, Section 5.

U.S. National Cancer Institute, “GDC Policies,” https://gdc.cancer.gov/about-gdc/gdc-policies.

U.S. National Institutes of Health. “Using Genomic Data Responsibly.” https://sharing.nih.gov/accessing-data/accessing-genomic-data/using-genomic-data-responsibly.

U.S. National Oceanic and Atmospheric Administration. “Cooperative Observer Program.” https://www.weather.gov/coop/Overview.

U.S. Supreme Court, *Carpenter v. United States*.

U.S. Supreme Court, *Smith v. Maryland*.

U. S. Supreme Court , *United States v. Miller*.

Verhulst S. and A. Young. “Battling Ebola in Sierra Leone: Data Sharing to Improve Crisis Response.” *Open Data’s Impact*, January 2016.

Verhulst, S., A. Young and P. Srinivasan. “An Introduction to Data Collaboratives: Creating Public Value By Exchanging Data.” https://datacollaboratives.org/introduction.html#learn-more.

Zingales, N. “Data Collaboratives, Competition Law and the Governance of EU Data Spaces,” in *Research Handbook on the Law and Economics of Competition,* ed. Ioannis Kokkoris and Claudia Lemus (Edward Elgar, 2022), 8–49.