Comparing Data Policy Priorities Around the World

By Gillian Diebold | September 5, 2023

Instead of duplicating any one approach, U.S. policymakers should borrow from the menu of options to craft a cohesive, pro-innovation data strategy.

INTRODUCTION

Common tropes about data, such as claims that it is the new oil, sand, or bacon, highlight data's growing importance to the economy and society. Many countries have responded by creating policies about data, including personal data, business data, and government data. These policies cover a range of issues, such as who can access it, where it can be stored, how it should be protected, and more.

There are important differences in how countries treat and value data. Some countries use data as an economic asset or as a tool for modernization and development, while others use data to exert control over citizens. This report compares key data policies in China, India, Singapore, the United Kingdom, and the European Union. These countries were selected to show the menu of options that countries have taken in data policy. Although the United States has created some important data policies, such as on open government data, it was not included because it lacks a clear and consistent national approach to key data policy issues, such as data protection where state legislatures have set many of the rules.

For each country, the report details the country's data policies' goals, strategies, and tactics, as well as the agencies involved. This report does not attempt to explore all the nuances of each country's data policies, particularly sectoral-focused policies in areas like financial services or health care. Instead, it focuses on broad, high-level thinking toward data. The report shows that while many countries recognize the social and economic value of data, the policies they pursue to maximize that value can vary widely.

Policymakers should learn from these global approaches and take action to craft a coordinated approach to data focused on two goals: maximizing the benefits of data-driven innovation (by encouraging data collection and data sharing, and avoiding unnecessarily burdensome data protection rules), and minimizing the barriers to cross-border data flows.

CHINA

China aims to build a strong internal data economy to strengthen national competitiveness and maintain government control over society through strict controls on the collection and use of data.

STRATEGIES

To build its data economy and society, China has three main data strategies:

- Maximize the use of data for economic growth by collecting as much data as possible for the benefit of the state.
- Closely monitor data about its citizens through state-run agencies.
- Promote economic nationalism to strengthen state control over data.

TACTICS

To support its strategies, China uses the following tactics:

- To maximize the economic benefits of data, China has classified data as a factor of production to cement its status as a key economic resource. National industrial policies now include directives for the allocation of data resources.
- To exert greater social control and monitor citizens, China limits anonymity online and requires the private sector to turn over data to the state, particularly in cases deemed important for national security.
- To promote economic nationalism, China limits the activities of foreign companies within its borders and requires all data to be stored domestically.

AGENCIES

China has two primary bodies that oversee data policies that advance digital development in the country:

- The Cyberspace Administration of China (CAC) oversees much of the country's digital regulations, including those on cybersecurity, data protection, cross-border data flows, and digital content. Originally falling under state administration in the Chinese system, the State Council reorganized the CAC in 2014 to have a merged party-state status which gives it less transparency and accountability.
- The National Data Administration (NDA) is responsible for data sharing between public institutions, data interconnection between large Internet platforms, and enabling private sector data use.

POLICIES

1. Classify data as a factor of production

   a. The **14th Five-Year Plan for National Informatization** details a number of projects to increase data collection based on the assertion of "the driving and leading role of informatization in economic and social development." [1] The plan explains the need to "fully express the crucial role of data as a new production factor…with whole-lifecycle governance and security protection as focus points." As a result, national industrial policies consider and include data resources.

2. Use data to exert greater social control

   a. The **Data Security Law (DSL)** empowers the state with heavy oversight authority. Article 21 establishes a classification system for data based on its potential impact on Chinese national security, with economic and security data afforded the highest level of protection. [2]

   b. The Cyberspace Administration of China has ultimate oversight authority for data protection and can impose fines, as well as suspend businesses and freeze assets, for violations, according to Article 45 of the DSL.

   c. The **Cybersecurity Law (CSL)** allows law enforcement access to personal data through mandatory backdoors.[3] Article 28 states that "network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities."

   d. The CSL also prohibits anonymity online. Article 24 states that "network operators…shall require users to provide real identity information…where users do not provide real identity information, network operators must not provide them with relevant services."

3. Promote economic nationalism

   a. The CSL provides regulations for cybersecurity and data protection to "promote the healthy development of the informatization of the economy and society." [4] Article 37 states that: "Critical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, shall store it within mainland China." Additionally, CSL requires business data and data on Chinese citizens collected within China to be stored within China and restricts its export.

   b. The **Personal Information Protection Law (PIPL)** strengthens personal data protection policies.[5] The PIPL focuses on keeping Chinese personal data within the country's borders. Section III of the law specifies that personal data held by state agencies must be stored within China's borders. Likewise, Article 38 lays out the strict conditions for cross-border transmission of personal data, namely a state-led security assessment.

[1] DigiChina, "Translation: 14th Five-Year Plan for National Informatization," Originally published December 28, 2021, https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/.
[2] DigiChina, "Translation: Data Security Law of the People's Republic of China," June 29, 2021, https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/.
[3] DigiChina, "Translation: Cybersecurity Law of the People's Republic of China," June 29, 2018, https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.
[4] Ibid.
[5] DigiChina, "Translation: Personal Information Protection Law of the People's Republic of China," August 20, 2021, https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.

INDIA

India aims to use data policy to spur modernization and development and unlock a new economic resource.

STRATEGIES

To achieve its modernization and development goals, India has three strategies:

- Strengthen consumer data privacy.
- Promote economic nationalism to bolster domestic actors.
- Harness nonpersonal data for economic growth.

TACTICS

India supports its strategic initiatives in the following ways:

- To strengthen consumer data privacy, India has proposed a personal data protection law that enhances individual privacy using purpose limitation and data minimization requirements while still laying out clear guidelines for using personal data. It also has a state-led suite of technology applications that centralize user consent agreements.
- To promote economic nationalism and bolster domestic actors, India supports data localization and the prioritization of Indian businesses accessing user data.
- To harness the value of nonpersonal data, India has created a national data sharing framework and created high-value datasets in critical areas.

AGENCIES

India regulates and monitors data with a mostly centralized approach led by its Ministry of Electronics and Information Technology (MEITy).[1] MEITy's mission is for the "e-Development of India as the engine for transition into a developed nation and an empowered society." Pending policies would also create new institutions to govern personal and nonpersonal data.

POLICIES

1. Strengthening consumer privacy
   a. The proposed **Digital Personal Data Protection Act** frames the rights of Indian citizens and the lawful use of personal data.[2] The most recent draft includes data minimization and purpose limitation requirements, but states that "The purpose of this Act is to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process personal data for lawful purposes."
2. Establish a state-led data fiduciary service
   a. The India Stack is a set of programs that strengthen the nation's digital infrastructure.[3] In addition to enabling data sharing for citizens using e-commerce and e-government services, the India Stack's consent layer, the **Data Empowerment Protection Architecture (DEPA)**, gives citizens greater autonomy over their personal data by establishing data fiduciaries who act as an intermediary between information users and providers and provide consent for companies based on a standard set by the user.
3. Promote India-first data sharing and storage
   a. Section 5.1 of the draft **Nonpersonal Data Governance Framework** includes the need for "benefits to accrue to relevant Indian communities; not only to the organizations that collects such data, but also equally to the community that typically produces the raw / factual data that is being captured…[including] with citizens, Indian start-ups, Indian companies, Indian public and private universities, Indian public and private research labs, Indian Non-Government organizations, and the Indian Central and State Governments."[4]
   b. Section 6 of the Nonpersonal Data Governance Framework mandates data sharing with a new horizontal category of Indian "data businesses" when there is a public interest rationale, like in the case of energy data or ride services and traffic. Section 6.3.v states that "Indian citizens and India-based organizations will have open access to the meta-data about data collected by different Data Businesses including governments." In the section's key takeaways, the report states that "The Committee strongly believes that meta-data sharing by Data Business will spur innovation at an unprecedented scale in the country… One of the associated key objectives is to promote and encourage the development of domestic industry and startups that can scale their data-based businesses."[5]
   c. Past drafts of the Personal Data Protection Bill included strict data localization requirements. The newer version of the bill released in August 2022 allows cross-border transfer and storage of data in "trusted" countries.
4. Enable non-personal data sharing
   a. The Nonpersonal Data Governance Framework covers data sharing for all types of non-personal data, including data entirely unrelated to people or personal data that has been anonymized, with the goal of enabling a data sharing framework that unlocks the "economic, social, and public value of data," addresses potential harms, and builds a national data repository from business and government.[6]
5. Create high-value datasets
   a. The Non-personal Data Governance Framework would establish two offices, an India Data Management Office, to develop new policies, and a Nonpersonal Data Authority to supervise data-sharing activities and approve applications for new high-value datasets. 7.2.ii in the framework recommends that "India should specify a new class of data at a national level…data of special public interest or high-value dataset, like health, geospatial and/or transportation data" and "progressively identify other priority sectors for harnessing the economic and societal benefits from leveraging non-personal data."[7]

[1] "Functions of Ministry of Electronics and Information Technology," Ministry of Electronics and Information Technology, last modified July 19, 2023, https://www.meity.gov.in/about-meity/functions-of-meity.
[2] Digital Personal Data Protection Act, Republic of India (2023), https://www.meity.gov.in/data-protection-framework
[3] "Data," India Stack, accessed July 2023, https://indiastack.org/data.html
[4] "Report by the Committee of Experts on Non-Personal Data Governance Framework," MEITy, Government of India, 2020, https://ourgovdotin.files.wordpress.com/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf.
[5] Ibid.
[6] Ibid.
[7] Ibid.

SINGAPORE

Singapore aims to use data as a vehicle to attract new businesses to operate within the country.

STRATEGIES

To achieve its goal of attracting new business, Singapore:

- Supports businesses in their use of data.
- Values the collection, sharing, and use of nonpersonal data.
- Protects consumer data with clear rules for compliance.

TACTICS

Singapore supports these strategies in the following ways:

- To support businesses and attract new enterprise, Singapore encourages organizations to use personal data for business innovation.
- To enhance the use and collection of nonpersonal data, Singapore creates data sharing frameworks that specifically facilitate data sharing between enterprises within the country.
- To protect consumer data, Singapore empowers individuals to advocate against negative business practices and put their data to use.

AGENCIES

The Infocomm Media Development Authority (IMDA) leads Singapore's data policy as the primary information and media regulatory body. Under its jurisdiction is the Personal Data Protection Commission (PDPC), which specifically enforces and administers the country's personal data protection law.

POLICIES

1. Enable enterprises to use personal data

   a. The goals of the Personal Data Protection Act (PDPA) include maintaining trust with citizens and "regulating the flow of personal data among organizations… to strengthen Singapore's position as a trusted hub for businesses."[1]

   b. The PDPA requires notification and consent of data collection but also creates exceptions for organizations in the case of legitimate public interest or for business improvement purposes. An update to the regulation in 2021 creates a "legitimate interests exception" in which businesses can collect, use, or disclose personal data without consent in certain situations.

2. Protect consumer interest within a pro-business framework

   a. Article 480 of the PDPA includes a private right of action for individuals against businesses that violate the PDPA, stating that "a person who suffers loss or damage directly as a result of a contravention…has a right of action for relief in civil proceedings in a court."

   b. The PDPC is in the process of updating regulations to include a **Data Portability Obligation (DPO)** in which an organization must transmit the individual's data that they possess to another organization in a common, machine-readable format.[2] Notable exceptions include "personal data which, if disclosed, would reveal confidential commercial information that could…harm the competitive position of the organization." Moreover, the DPO only requires porting to organizations originating or with offices in Singapore.

3. 3. Facilitate B2B data sharing

   a. IMDA created the Trusted Data Sharing Framework to facilitate B2B data sharing for both personal and nonpersonal data.[3] It aims to create a systemic approach to data sharing, given that "the motivation to share data typically stems from business needs." The framework provides a "common data sharing language" and includes sample legal templates for contractual data sharing.

[1] "PDPA Overview," Personal Data Protection Commission Singapore, accessed July 2023, https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act.
[2] "Upcoming Changes to the PDPA: Introducing Data Portability," PK Wong & Nair, October 26, 2022, https://pkwongnair.com/2022/10/26/upcoming-changes-to-the-pdpa-introducing-data-portability/.
[3] "Trusted Data Sharing Framework," Infocomm Media Development Authority, last modified August 3, 2023, https://www.imda.gov.sg/how-we-can-help/data-innovation/trusted-data-sharing-framework.

UNITED KINGDOM

The United Kingdom (UK) aims to boost national economic competitiveness while protecting its citizens' data privacy.

STRATEGIES

To support its goal of protecting citizens while bolstering national competitiveness, the UK uses the following strategies:

- Promote privacy in a user-friendly manner, meaning that personal data is both protected and accessible.
- Attract new businesses to operate in the country and support existing enterprises.
- • Enable innovation through a regulatory environment that supports development and experimentation.

TACTICS

The UK uses the following tactics:

- To promote user privacy and accessibility of user data, the UK has clear data protection rules and facilitates the use of data by both users and businesses.
- To attract new businesses and support existing ones, the UK plans to increase industry access to data through better reuse of public sector data and enhanced data sharing mechanisms.
- To enable innovation, the UK has developed a flexible regulatory environment through the use of regulatory sandboxes which allow companies to try out new products and services on real consumers in a controlled environment without risk of regulatory penalty.

AGENCIES

The UK takes a horizontal approach to data protection regulation, whereas it uses a sectoral approach for data sharing regulation. The Information Commissioner's Office (ICO) is an independent government body specifically governing data protection and data sharing guidelines.[1]

POLICIES

1. Re-balance user privacy and innovation

   a. Through various legislation, including the **UK GDPR, Data Protection Act (DPA),** the **Privacy Electronic Communications Regulations**, and the proposed **Data Protection and Digital Information Bill**, the UK covers core data privacy principles.[2] This includes things like data portability requirements, business access to personal data, and the flow of data for law enforcement purposes.

   b. The **Pro-innovation Regulation of Technologies Review: Digital Technologies**, states that "Ensuring a proportionate and agile regulatory approach can offer clarity and confidence to investors, businesses and the public."[3] It acknowledges the perception of the UK's privacy regime as "restrictive," and outlines recommendations for greater balance, stating that "there needs to be an appropriate balance between the assessment of risk and benefit."

2. Reuse public sector data

   a. Part 5 Chapter 1 of the **Digital Economy Act** provides rules for data sharing between public bodies, such as for the production of statistics, for research purposes, for public service delivery like utilities, or for debt and fraud cases.[4]

   b. The review of digital technologies states that "the government and broader public sector bodies hold significant data, which if made available to industry in a consistent way, could facilitate research and innovation and improve public services," and recommends prioritizing linkage of industry with public sector data.

3. Enhance data sharing mechanisms

   a. The **ICO Data Sharing Code** offers best practices for data sharing for organizations that handle personal data.[5] Emphasizing the importance of data sharing mechanism, the code states that "data sharing can sometimes be a complex activity. But in some organizations, the perceived risks of getting it wrong… outweigh the benefits that can be gained from data sharing, leading to missed opportunities for innovation."

   b. The **Second Payment Services Directive (PSD2),** combined with the UK Competition and Markets Authority rules on **Open Banking**, requires national banks to make their data available in a standardized format.[6] This way, third parties can use the information to create new products and services.

4. Develop regulatory sandboxes

   a. The review of digital technologies also lays out the importance of regulatory flexibility in adopting a "pro-innovation approach that facilitates widespread adoption of commercial science and technology applications."[7] It specifically recommends that "government should work with regulators to develop a multi-regulator sandbox for AI to be in operation within the next six months."

[1] "About the ICO," Information Commissioner's Office, accessed June 2023, https://ico.org.uk/.
[2] Regulation (EU) 2016/679 of the European Parliament and of the Council (UK GDPR), April 27, 2016, https://www.legislation.gov.uk/eur/2016/679/contents and Data Protection Act, 2018, https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.
[3] Patrick Vallance, "Pro-innovation Regulation of Technologies Review — Digital Technologies," HM Government, March 2023, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/114 2883/Pro-innovation_Regulation_of_Technologies_Review_-_Digital_Technologies_report.pdf.
[4] Data Protection Act, 2018, https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.
[5] "Data sharing: a code of practice," ICO, accessed June 2023, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/.
[6] "Payment Services Directive 2 and Open Banking," UK Finance, accessed June 2023, https://www.ukfinance.org.uk/policy-and-guidance/guidance/payment-services-directive-2-and-open-banking.
[7] Patrick Vallance, "Pro-innovation Regulation of Technologies Review — Digital Technologies," HM Government, March 2023, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/114 2883/Pro-innovation_Regulation_of_Technologies_Review_-_Digital_Technologies_report.pdf.

EUROPEAN UNION

The European Union (EU) uses a human rights-based approach to data protection that prioritizes a single market for the free flow of data among member states.

STRATEGIES

To achieve its high-level agenda, the EU:

- Prioritizes the pursuit of human rights over economic interests.
- Enables digital transformation within the region.
- Uses data to increase social and economic benefits for residents.

TACTICS

The EU uses the following policy tactics to achieve its goals:

- To prioritize individual users, the EU creates a number of data and digital rights with strict enforcement measures. It also sets design mandates for manufacturers.
- To enable digital transformation, the EU sets concrete targets for key digital milestones.
- To increase social and economic benefits, the EU facilitates data sharing for public and private actors.

AGENCIES

The EU has two supranational oversight boards:

- The European Data Protection Board (EDPB) oversees the application of data protection regulations. It comprises national data protection authorities and the European Data Protection Supervisor, the EU's independent supervisory authority.
- The European Data Innovation Board establishes data-sharing policies and oversees data altruism organizations.

POLICIES

1. Enshrine data and digital rights

   a. The **General Data Protection Regulation (GDPR)** is the most stringent data protection law in the world. It provides a large list of requirements for organizations regarding what they can do with the personal data of individuals in the European Union. There are seven data protection principles: lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability.

   b. The **Digital Decade** program includes a declaration of digital rights and principles for individuals in the EU which complement their existing data and privacy rights. Its **Declaration on Digital Rights and Principles** states that "with the acceleration of the digital transformation, the time has come for the EU to spell out how its values and fundamental rights applicable offline should be applied in the digital environment. The digital transformation should not entail the regression of rights."

2. Mandate data sharing by design

   a. As part of the **European Strategy for Data**, the **Data Act** includes a data sharing by design obligation for manufacturers that enhances user access and rules pertaining to data processing services, such as international transfer of non-personal data and interoperability requirements.

3. Create digital milestones

   a. The Digital Decade program sets concrete targets for digital transformation to meet by 2030. It focuses on using data in multi-country projects to help meet these targets, which relate to digital skills, business transformation, digital infrastructure, and digital public services. These projects "support an interconnected, interoperable and secure Digital Single Market."

4. Establish common European data spaces

   a. The other piece of legislation under the European Strategy for Data, the **Data Governance Act (DGA)**, creates "common European data spaces" organized by data intermediaries tasked with safeguarding the data. These data spaces are in strategic domains, specifically: health, environment, energy, agriculture, mobility, finance, manufacturing, public administration, and skills. According to the European Commission, "the framework offers an alternative model to the data-handling practices of the Big Tech platforms, which have a high degree of market power because they control large amounts of data."

5. Enable other forms of data sharing: Data altruism

   a. The DGA enables altruistic data sharing, meaning individuals and certain businesses can donate their data for the public interest. The goal of data altruism is to "create trusted tools that will allow data to be shared in an easy way for the benefit of society."

[1] "General Data Protection Regulation," Intersoft Consulting, accessed June 2023, https://gdpr-info.eu/.
[2] DECISION (EU) 2022/2481 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, establishing the Digital Decade Policy Programme 2030, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022D2481&from=EN.
[3] "European Declaration on Digital Rights and Principles," European Commission, February 7, 2023, https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles.
[4] "A European Strategy for data," European Commission, last modified June 19, 2023,https://digital-strategy.ec.europa.eu/en/policies/strategy-data.
[5] "Europe's Digital Decade: digital targets for 2030," European Commission, accessed August 2023, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en#multi-country-projects.
[6] "Data Governance Act explained," European Commission, last modified August 9, 2023, https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained.
[7] Ibid.
[8] Ibid.

ANALYSIS AND TAKEAWAYS

Data policy has become a priority for many countries as they seek to maximize the social and economic benefits of data. A government's approach to data policy signals its priorities and interests and likely indicates how it will act toward future data-related issues. Although each country's policies are fluid—changing over time in response to new developments, changes in government leadership, and shifting priorities—distinct trends tend to emerge on issues of data protection, data sharing, and access to data.

Some countries' purported goals can sometimes be at odds with their actual policies. For example, the European Union has produced many statements declaring its commitment to promoting data-driven innovation, yet it also has significantly restricted data sharing with its data protection law. Likewise, China passed data protection legislation that applies to private sector collection and use of personal data but allows near-total government access.

Data protection has long been a top priority for data policy, however, in recent years, more policymakers have begun to recognize that there are tradeoffs between data protection and innovation. As a result, some countries seek to balance protecting data from misuse with ensuring data can be used to create economic and social value. For example, India has data security protections for its citizens that coexist with regulations to expand the use of personal and nonpersonal data. Similarly, Singapore's data protection law has sought a more balanced approach than the EU's GDPR, discarding the data minimization principle and making it easier for organizations to collect and use personal data. Likewise, the UK's proposed Data Protection and Digital Information Bill has more permissive provisions than the GDPR to allow business and law enforcement access to personal data. In contrast, the European Union's approach prioritizes individual rights, and all subsequent legislation works to make data sharing feasible within the confines of the GDPR. China's data protection rules also impose significant restrictions on how the private sector can handle personal data but do little to limit the central government from accessing this data.

Many countries have also created policies to promote data sharing. Some countries prioritize collaborative data sharing arrangements between industry and government actors, while others solely focus on data sharing with or within the government itself. For example, India's Nonpersonal Data Governance Framework creates a set of rules and obligations for businesses and the government to follow when sharing data to spur innovation and bolster its domestic startup economy. Along similar lines, the UK's Digital Economy Act enables the public sector to share data with industry, given its view that the private sector is best equipped to extract economic value from data. Singapore removes government from the equation and focuses on facilitating B2B data sharing for personal and nonpersonal data, in line with its business-first approach.

Some countries aim to use data policies to exert greater social control. For example, China created its National Data Administration to focus on inter-governmental data sharing. China also mandates one-way data sharing from large Internet platforms, justifying this policy by citing national security. But this type of arrangement stifles business operations even if bolstering the domestic economy is a key goal for some countries.

Controlling or enabling access to data is another way countries can achieve their strategic goals. Some countries view domestic access to data as a vehicle for boosting national competitiveness. For example, China and India both promote economic nationalism via data localization measures that

require domestic storage of data. Although countries like the EU and China disagree on the method and reasoning for data control, both still engage in similar activities. The EU restricts foreign access to data but allows domestic access to data and the flow of data within its borders. It sets strict rules for the collection, use, and transfer of data and prohibits the transfer of EU data to any country that does not adopt data protection rules equivalent to the GDPR. By restricting cross-border data flows, the EU can impose its digital rights-oriented approach to data protection on other nations.

Some countries, like India, have used public digital infrastructure to guide data policy implementation. Through its India Stack suite of technology, India enables more e-commerce and e-government services through its public-facing digital platform. Moreover, its Data Empowerment and Protection Architecture (DEPA) is a layer of the tech stack specifically designed to facilitate user consent and general transparency of data collection practices. DEPA establishes a framework for apps and digital services to use when collecting data in which individuals can grant explicit and granular permission for data use. It mandates organizations to provide clear and concise explanations of how data is being used.

Notably, while most countries recognize that data is necessary for product development, service delivery, and evidence-based policymaking, few have taken steps to create proactive policies to produce more high-value data. Countries need to engage in active conversations with the private sector to identify what data would be most valuable to collect and produce or where data gaps exist that the public sector could fill. India's Nonpersonal Data Governance Framework enables the creation of datasets in high-value areas and is one way to tackle the data production issue proactively.

Moving forward, countries should create a coherent strategy that covers these core components of data policy, namely data protection, data sharing, data access, and data production. Countries also need to think through what goals they are trying to achieve through data and avoid creating contradictory policies. Consider the EU: although European policymakers want to increase social and economic benefits for residents and support a Digital Single Market, most of the EU's policies restrict data usage and impose costly requirements on businesses. These requirements include GDPR compliance, device design mandates, and data-sharing mechanisms that disallow private sector involvement. When designing national-level data strategies, countries need to be aware of such contradictions to ensure cohesive policies.

Countries that aspire to be leaders in the AI economy need to take a pro-innovation approach to data policy that balances data protection with the economic and social benefits that come from data collection and use. More specifically, an ideal data policy framework that takes a pro-innovation approach should include:

- *Risk-based data protection.* Risk-based approaches to data protection encourage organizations to focus on protecting sensitive personal data, such as an individual's medical history or financial information, while reducing regulatory costs for non-sensitive data.[1] Data protection rules should still provide users with the ability to access, port, delete, and rectify their data, even sensitive data, within certain limits, and should not include data minimization or purpose specification requirements which limit innovation.

[1] Ashley Johnson and Daniel Castro, "Maintaining a Light-Touch Approach to Data Protection in the United States" (August 2022), https://itif.org/publications/2022/08/08/maintaining-a-light-touch-approach-to-data-protection-in-the-united-states/.

- *Data sharing frameworks for personal and nonpersonal data*. Countries should foster data sharing by both the private and public sector of both personal and nonpersonal data. Rules should enable data sharing by default, reduce regulatory barriers to voluntary data sharing, and eliminate intra-governmental red tape to data sharing.
- *Free flow of data.*[2] Countries should facilitate cross-border data flows to foster digital free trade. Countries should not impose data localization requirements and should promote an open, competitive, and rules-based global digital economy.
- *Proactive data production policies.*[3] Countries should prioritize data as a key factor of production in their economies. To that end, countries should promote data collection across sectors and invest in data production to spur innovation and avoid harmful data gaps.

A pro-innovation data strategy for the United States

Instead of duplicating any one approach, U.S. policymakers should borrow from the menu of options to craft a cohesive, pro-innovation data strategy. Such a strategy should include:

Comprehensive data privacy legislation that takes a targeted, risk-based approach. Data protection regulations in the United States presently exist on a state-by-state basis, creating a patchwork of laws that are confusing and costly. Proposals for a national bill, including the American Data Privacy and Protection Act (ADPPA), make important strides, but need some key adjustments to preempt state laws, distinguish between sensitive and nonsensitive personal data, and exclude a private right of action.

Plans for a National Data Foundation to facilitate increased data sharing. The United States needs data sharing to be the norm, rather than the exception. Establishing a National Data Foundation would allow the government to invest in data in a similar way to how it invests in science. In addition, a National Data Foundation could create technical standards, governance frameworks, and best practices for sharing various types of data. Moreover, such a foundation can play an important role in coordinating an increase in the production and collection of data nationwide.

Commitments to the free flow of data across borders. Allowing the free flow of data across borders aligns with the United States' democratic principles and recognizes that data flows are a force for good. The United States should resist efforts by countries seeking to impose their data policies on other countries, as well as oppose restrictions on cross-border data flows, including in fora such as the US-EU Trade and Technology Council.

[2] Nigel Cory, "In the Global Battle Over Data Flows, Data Liberals Must Fight Back Against Data Nationalists and Interventionists," *Global Trade*, June 17, 2022, https://www.globaltrademag.com/in-the-global-battle-over-data-flows-data-liberals-must-fight-back-against-data-nationalists-and-interventionists/.

[3] Gillian Diebold, "The United States Can Learn from China's New National Data Administration," Center for Data Innovation, April 12, 2023, https://datainnovation.org/2023/04/the-united-states-can-learn-from-chinas-new-national-data-administration/.

Country	Data Protection?	Data Sharing?	Data Access?	Data Production?
China	**Yes.** The Data Security Law (DSL) and Personal Information Protection Law (PIPL) create data protection obligations for private enterprise, but China does not restrict government access to data.	**Yes, between public institutions.** The National Data Administration mandates one-way data sharing from large Internet platforms with government bodies.	**Data Nationalist.** The Cybersecurity Law (CSL) requires data from businesses operating in China to be stored domestically and prohibits its transfer abroad.	**Yes.** Including data resources in national industrial policies signals a proactive interest in data collection for all areas.
India	**Not yet.** India has yet to pass comprehensive personal data protection legislation, but a draft bill is under consideration.	**Yes, especially nonpersonal data.** The Nonpersonal Data Governance Framework enables a national data sharing framework that contributes to a national data repository.	**Remains to be seen.** Draft legislation has historically included strict data localization requirements, but newer versions allow cross-border transfer and storage in "trusted" countries.	**Yes.** The Nonpersonal Data Governance Framework would create a national dataset of special public interest in fields like healthcare or transportation data.
Singapore	**Yes.** The Personal Data Protection Act (PDPA) regulates the collection of personal data while enabling the use of personal data for business purposes.	**Yes, between businesses.** The Trusted Data Sharing Framework facilitates B2B data sharing and provides contractual templates for businesses.	**Data Liberal.** Singapore supports the free flow of data across borders.	**No.**
United Kingdom (UK)	**Yes.** A number of bills cover core data protection principles.	**Yes.** The Digital Economy Act provides rules for data sharing between public bodies. The UK also leads on Open Banking, i.e., the sharing of financial data.	**Data Liberal.** The UK supports the free flow of data and aims to attract new business using regulatory sandboxes.	**No.**
European Union (EU)	**Yes.** The General Data Protection Regulation (GDPR) uses a human-rights based approach with stringent data protection requirements.	**Yes, in some cases.** The creation of common European data spaces enables data sharing within the regions borders. Data altruism provisions enable data sharing but exclude private firms from participation.	**Data Interventionist.** Data flows are conditioned on other countries harmonizing their privacy rules to fit EU preferences via "adequacy" requirements.	**No.**

ABOUT THE AUTHOR

Gillian Diebold is a Policy Analyst at the Center for Data Innovation, focusing on data policy and digital inequalities. She holds a B.A. from the University of Pennsylvania, where she studied Communication and Political Science.

ABOUT THE CENTER FOR DATA INNOVATION

The Center for Data Innovation studies the intersection of data, technology, and public policy. With staff in Washington, London, and Brussels, the Center formulates and promotes pragmatic public policies designed to maximize the benefits of data-driven innovation in the public and private sectors. It educates policymakers and the public about the opportunities and challenges associated with data, as well as technology trends such as open data, artificial intelligence, and the Internet of Things. The Center is part of the Information Technology and Innovation Foundation (ITIF), a nonprofit, nonpartisan think tank.

Contact: info@datainnovation.org

datainnovation.org