
CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE
AUGUST 2022
Data Governance, Asian Alternatives
How India and Korea Are Creating New Models and Policies
Evan A. Feigenbaum and Michael R. Nelson, editors
Rahul Matthan | Taewoo Nam | Kyung Sin "KS" Park | Smriti Parsheera | Shreya Ramann

Data Governance, Asian Alternatives

How India and Korea Are Creating New Models and Policies

Evan A. Feigenbaum and Michael R. Nelson, editors
Rahul Matthan | Taewoo Nam | Kyung Sin "KS" Park | Smriti Parsheera | Shreya Ramann

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

CONTENTS

Project Participants

The volume's editors are grateful to the participants in a virtual workshop on "India, Korea, and the Future of Data," and they are especially appreciative of those who offered helpful comments on chapter drafts. They also express thanks to the Korea Foundation for its generous support of this project.

Bishakha Bhattacharya
Amazon India (and South Asia)

Anirudh Burman
Carnegie India

Anupam Chander
Georgetown University

Bonnie Carroll
CENDI

Mila Gascó-Hernandez
University at Albany

Young Hoon Kim
Amazon Korea

James Miller
Amazon Japan

Joshua New
IBM

Lorrayne Porciuncula
Internet and Jurisdiction Policy Network

Upasana Sharma
Carnegie India

Paul Uhlir
Information Policy and Management Consultant

Naomi Wilson
Information Technology Industry Council

INTRODUCTION

How India and Korea Can Drive New Thinking About Data

EVAN A. FEIGENBAUM AND MICHAEL R. NELSON

Deepening concerns about digital authoritarianism have led many observers to posit that a stark contest between democracy and autocracy is poised to shape the governance of technology and data.[1] In this reckoning, the world's democracies are said to have open approaches that rely on market mechanisms. By contrast, the world's autocracies privilege the role of the state and aim to strengthen its capacity to harness all data, both public and private.

But this binary framing elides the extent to which democracies have developed diverse approaches. Some democracies, especially in Asia, have adapted policy and regulatory features that deepen and extend the reach of the state. Some democracies, again especially in Asia, have developed data governance regimes that reflect the unique features of their institutions and political cultures.

It is important, therefore, to dig into this diversity, especially at a moment when there is a growing focus on data policy at both the international and national levels. This intensifying focus on data is being driven by several factors, including

- the growing power of multinational cloud services companies, such as Amazon Web Services;
- the extraordinary amounts of data being collected by social media platforms;
- the growing importance of the Internet of Things in many sectors of the global economy;

- widespread fears around the world that citizens' data are being siphoned off for the benefit of foreign companies;

- the essential role that data used for contact tracing and quarantine restrictions played in mitigating the impact of the coronavirus pandemic; and

- excitement around new applications of artificial intelligence (AI), especially machine learning, which will benefit companies and countries able to generate, manage, and remix gigantic stores of high-quality data.

Amid this growing focus on data, the world is *not* fracturing into just two spheres—an autocratic Sinosphere dominated by China and an open, democratic sphere centered on the transatlantic West. Instead, *third* countries, many of which are consolidated democracies, are influencing debates about data policy, the business models of technology firms, and regulatory frameworks. If these countries can collaborate, leverage the power of open standards and open-source software, and demonstrate new approaches to digital development, they could become leaders in their own right as the next phase of the data economy unfolds.

This volume highlights some of the alternative models that have originated in two major Asian democracies, India and South Korea (hereinafter Korea). It compares these two countries' distinctive approaches through case studies that demonstrate just how much more complex the world will be than the commonplace prediction of a battle between U.S.- and Chinese-centric approaches.

This volume is a sequel to a 2021 study, *The Korean Way With Data,* a multichapter deep dive into three critical aspects of Korea's distinctive experiences with data: data resilience, data localization and privacy, and online authentication and data access control. This follow-up volume extends and expands that earlier stream of work by explicitly comparing Korea's experience in two areas—open data and cross-border data governance—with that of India, a leader in software and information technology (IT) services.

Bluntly put, to those who believe that the world faces a stark or binary choice between transatlantic-centered democratic models or China-centric authoritarian ones, this volume should be an eye-opener. Like the 2021 volume on Korea, this study demonstrates that additional players are leading the way in several key respects. Both India and Korea are consolidated democracies, and neither of them is simply emulating U.S. or European experiences. Instead, they are pioneering their own approaches, mixing and matching elements of their unique democratic institutional frameworks with national requirements and policies derived from distinctive political cultures.

To be sure, progress on data governance in both India and Korea has been uneven. Their stories are by no means simple ones. For example, this volume shows that different agencies in the governments of each of these countries have conflicting policy goals and, when their preferred policies have collided, it has proved almost impossible to develop a clear, consistent vision and strategy. The result has been inadequate investment; stalled-out projects; and missed opportunities to share, combine, and use data to solve problems in the Indian and Korean public and private sectors.

When Policies Collide

An important theme that links both the 2021 and 2022 volumes is that disparate agencies in a fragmented bureaucracy can lead to disparate policy goals. The two chapters in this volume by Korean authors (along with a chapter in *The Korean Way With Data* by Nohyoung Park) highlight inconsistencies and points of conflict and competition across the Korean bureaucracy in Seoul.[2]

At international fora such as the Group of 20 (G20), Korea's Ministry of Foreign Affairs has worked hard to forge agreements to facilitate cross-border flows of data. The ministry's efforts have been supported by the Korean Ministry of Economy and Finance, which strives to maximize opportunities for Korean firms that want to provide data-driven services to customers and companies around the world. But at the same time, Korea's national security agencies have blocked the export of certain types of map data and other data that they judge could be used by North Korea or other adversaries to attack South Korea. These security-focused agencies fret not just about physical attacks but also malicious hacks and information warfare (including disinformation). Meanwhile, Korea's financial regulators and various government agencies tasked with protecting the privacy of Korean citizens' personal data are leery about allowing foreign companies to store and process Korean data in other countries, particularly in countries with inadequate, unclear, or poorly enforced data protection regulations.

The situation is quite similar in India. The country's Ministry of Electronics and Information Technology has championed the cause of a "borderless" digital world so that Indian firms can move data easily across borders and better serve their customers, no matter where they happen to be located.[3] But as Smriti Parsheera shows in her chapter in this volume, there are many barriers to realizing this Indian vision for cross-border data. As in the case of Korea, these obstacles include objections from India's privacy regulators, who are developing Indian data protection rules that could block the export of Indian citizens' personal data to other countries.

Even more serious are the demands of Indian law enforcement agencies, which want access to data to conduct criminal investigations and ensure regulatory compliance. These agencies fear that if Indians' data are stored overseas, whether in corporate databases, social media platforms, or cloud computing centers, they will struggle to gain access to the data they want.

But India and Korea do diverge in one respect: in India, these arguments from law enforcement often seem to win the day. In Korea, by contrast, national security concerns have had a much greater impact on outcomes and policies than the concerns of law enforcement have.

The Need for Digital Leadership

Interestingly, in both India and Korea, digital policy sits atop the list of national priorities. That is why both countries' governments are tackling digital and data-related issues at the highest possible level. India's Prime Minister Narendra Modi made the Aadhaar biometric identity project, which has given hundreds of millions of Indians a form of digital identification, a *personal* priority. Similarly, in the 2022 Korean

presidential election, the major parties' candidates debated the topic of digital identity (and the failures of earlier national efforts). This is not typical of most countries today. This provides yet another reason why Korean and Indian efforts to craft digital policies deserve much more attention globally than they have hitherto received.

Countries whose presidents and prime ministers take the lead on policy decisions related to the digital economy often force competing ministries to forge a consensus. These countries end up with a huge advantage in helping data-intensive industries compete. Ultimately, these countries tend to fashion new e-government solutions, foster machine learning, and enable new, data-driven business models.

Just take Estonia, a much smaller economy than either India or Korea: it has benefited hugely from the digital leadership shown by former president Toomas Hendrik Ilves, who became an internationally respected champion for e-government and cybersecurity policy.[4] In the United Kingdom, former prime minister Tony Blair's personal involvement in promoting e-government helped break through bureaucratic barriers that hindered agencies online, and the work of the Tony Blair Institute for Global Change is helping current leaders go digital.[5] In the United States, some have argued that the early successes of former president Bill Clinton's administration in promoting the commercial internet, which made the U.S. government a leader in using the World Wide Web and in fostering e-commerce, owed much to the powerful role played by the White House (and especially by then vice president Al Gore).[6] Gore and the White House took on a very high-profile role in crafting all-of-government strategies for the internet.[7] White House events, high-profile speeches, public relations campaigns, and demonstration projects (such as the White House's first website) also helped to highlight the need for proactive digital policies.[8] More recently, former president Barack Obama's personal participation in digital initiatives led him to be labelled the "Digitizer in Chief" and the "Geek-in-Chief."[9]

Today, in most countries, there is even more potential for digital innovation but less digital leadership. The result has been conflicting policies promulgated by different agencies that can discourage innovators and risk-takers in both the private sector and the government bureaucracies. These players want to offer new tools and online services but fear running afoul of government regulations regarding data protection, export controls, surveillance requirements, cybersecurity, and more. From a global perspective, the Indian and Korean experiences highlighted in the four chapters that follow are standouts.

Faulty Metaphors Can Lead to Faulty Policies

But, of course, leadership does not mean that presidents and prime ministers must delve deeply into the arcana of data management and technical standards for them to shape digital policy. In many cases, their most important contribution can simply be to share a vision for how information technology and the data it generates, collects, combines, and analyzes can benefit the citizens they govern and the countries they lead. Simply put, savvy national leaders can explain how to think about the digital future.

But unfortunately, too many policymakers have adopted faulty metaphors and models that only confuse their countries' thinking about data. The most obvious example is the frequent statement that "data is the new oil," which was popularized by a 2017 cover story in the *Economist*.[10] While it is certainly true that data is valuable like oil, in many ways this analogy is not only not useful but is even downright harmful.[11]

For one thing, comparing data to oil implies that data is a *commodity* to be sold and consumed. But data is not, in fact, a finite good that, like oil, is traded and shipped back and forth. Indeed, unlike oil and other commodities, it is simple to *replicate* and *share* data, increasing its use and value. The idea that data is a "fuel" for the digital economy is leading too many policymakers to assume that countries should hoard the data produced within their borders.[12] Even more misleading is the idea that data is "currency," implying that data should be either tightly controlled or traded, like a national currency, rather than shared jointly.[13]

What, then, is a better model? A simple one is that data is actually more like air or water than like either oil or currency.[14] Like air, for example, data can be viewed as something that should be allowed to flow *freely*, transcending national borders. That is because air, like data, can be used and reused for many different purposes by many different people. It can be polluted like the air, but it can also be cleaned. This approach to thinking about data—as air rather than as oil or a currency—works particularly well when addressing scientific data, such as environmental data, since researchers all over the world need it.

But water is another useful metaphor because for most data, there *are* reasons to place some limits on its use and flow. Reasons to do so can include data protection and privacy, national security, copyright enforcement, assuring commercial advantage, and others. In these cases, a different analogy can be used. Instead of flowing freely like air, such data should be treated like water.[15] After all, almost all the world's water circulates freely in oceans, rivers, lakes, and atmospheric clouds or is locked in cold storage in ice sheets and glaciers. But *some* of the world's water is captured in reservoirs, filtered, and piped to customers. And some water, usually from underground aquifers, is then bottled, branded, and sold.

For policymakers who want to put some limits on data, this water analogy works quite well. It effectively conveys how important data is to life in the digital age and how leaders need to work to ensure more clean data are made available to more people. Treating data like water makes it clear that not all data is the same or has the same value and, most importantly, that data is something—like water—that can be reused and remixed.

Key Choices for Policymakers

The critical top-level issue for policymakers wrestling with data policy is whether to try to create a single overarching approach to data management or instead to take a more federated approach.[16] To extend the water metaphor a bit further, the choice policymakers face is whether to have a single unified national water utility that serves every home, or instead to encourage the formation of multiple local water companies and home-based wells that operate within a broad regulatory framework.

In their chapter in this volume, Indian authors Rahul Matthan and Shreya Ramann explain how the Indian government is promoting a Data Empowerment Protection Architecture (DEPA) to consolidate data sets throughout the Indian government and beyond. But in Korea, as Taewoo Nam shows in his chapter, the government has encouraged hundreds of companies to work with different ministries to find new, useful ways to apply the data they collect. These two Asian democracies have thus arrived at two very different approaches.

From our perspective at least, the Korean approach that Nam describes is much easier to implement when companies are permitted to take full advantage of the many cloud service providers that can give even small or medium-sized companies access to powerful data storage, machine learning tools, and cybersecurity services. These were previously only available to large IT firms. But because many of these services are now provided by American or Chinese companies, countries that lack homegrown cloud services providers fear that foreign countries will not adequately protect the data they process. In the Chinese case especially, there are national security concerns that come into play because Beijing has an intrusive approach to data generally.[17]

As the following chapters make clear, law enforcement agencies, including those of India, are especially concerned that they will not be able to access the data they need to catch and prosecute criminals if that data is stored in data centers controlled by companies overseas. In the United States, similar concerns led to the Clarifying Lawful Overseas Use of Data Act (or the CLOUD Act), which specifies how foreign governments can request data from U.S.-headquartered cloud service providers.[18] But countries like Korea and India have not yet been able to benefit from this U.S. legislation.

There have, therefore, been calls in Korea and India for more data localization, motivated by both governments' desire to protect citizens' privacy and by India's aspirations to enable greater data access for law enforcement surveillance.

India in particular has benefited from Indian IT firms that process data for companies around the world. In the past, India has permitted the free movement of data across its borders, but pending domestic legislation would reverse these more open practices.[19] Similarly, in Korea, arguments for and against localization are becoming more pronounced, as Kyung Sin "KS" Park documents in his chapter in this volume. The few studies that have assessed the economic impact of data localization requirements have found that limiting cross-border data flows can significantly slow gross domestic product (GDP) growth.[20] How governments decide to balance economic benefits against other factors will help to define the future of the data economy. Park makes an important argument that the free flow of data should also be viewed as a human rights issue since citizens want to be able to choose which companies control and protect data about them and which governments might be able to access that data.

But this will require them to think differently and adopt some new approaches. One particularly exciting new model for data governance involves data unions or data cooperatives, an idea being promoted by U.S. computer scientist Sandy Pentland and his colleagues at the Massachusetts Institute of Technology among others.[21] A data cooperative functions like a bank or credit union, but rather than handling and distributing money, it stores and shares data about individual users. The key to making this model work

is that the cooperative is contractually obligated to users or users' organizations to protect and use data about an individual or group for that party's own benefit. The most important impact of this approach is that it would enable a very distributed data architecture, where data would not need to be pooled in a few data oceans controlled by just a small handful of companies.

The following chapters highlight the digital policy challenges governments are facing, and why these challenges are becoming increasingly complicated and ever more important. Indian and Korean experiences, models, and struggles can help digital policymakers around the world, especially in other raucous democracies, design their own governments' data policies.

Implications for Internet Governance

The main focus of this volume is what is happening in India and Korea at the national level and what other national policymakers can learn from their experiences. But there is another dimension to the volume—namely, how these models could influence debates in international fora about the future of the internet.

Internet governance is a broad term encompassing the full range of decisions, large and small, made by governments, corporations, standard-setting bodies, and users that affect how the internet operates and evolves.[22] For years, diplomats, technology policymakers, corporate representatives, and others have debated how these decisions are made and whether more international coordination is needed. Thousands of international meetings have been held, and an extensive literature has developed about these choices.

Today, these debates about internet governance are more important than ever. A key question is whether the internet will continue to be an open, global network connecting users everywhere or whether it will fragment into national and regional networks as governments exert more influence over how it is designed and how it is used.[23] A new and broader debate has also emerged about digital policy. Rather than just focusing on the networks that connect internet users to the applications they wish to use, the data and equipment attached to the internet, such as smartphones, Internet of Things devices, data centers, and cloud computing facilities are also drawing attention.

This growing attention is reflected in debates about international data governance, data sovereignty, and "the datasphere."[24] The secretary general of the United Nations (UN), António Guterres, has been promoting "digital cooperation," which builds on the work of the Internet Governance Forum and various UN agencies and offices but extends far beyond merely shaping the Internet and how it functions.[25] Much of the UN-related work Guterres has promoted focuses on data policy and the need to make high-quality data more available to more people for more purposes (with a special emphasis on fulfilling the UN's Sustainable Development Goals).

Placing more of a focus on data and how it can be applied could help remove the barriers that prevent innovators in countries around the world from developing and experimenting with new online services. This includes a wide array of activities ranging from conducting life-changing and life-saving research to

helping workers be more productive and energy-efficient and making lives safer and more secure. But in most countries, data policy has been an overlooked backwater. Unlike politically fraught issues like online privacy, hate speech on the internet, or disinformation and the polarization it causes, discussions about making government data more available or about cross-border data flows simply do not generate headlines. Worse, there are no easy answers to these policy questions because different types of data require very different types of treatment.

Most governments (including those of India and Korea) have no clear and singular focal point for data policy decisions. Internationally, there is similarly no such body as a World Data Organization (and most, including us, would argue against any such idea). Instead, there are many different intergovernmental organizations and scientific organizations that tackle different pieces of this data puzzle. At the highest level, for example, the G20 has added cross-border data flows to its agenda, not least through the late Japanese prime minister Abe Shinzo's push at the 2019 G20 Osaka Summit for "data free flow with trust." Abe's initiative led to the emergence in 2021 of the G7's Digital Trade Principles, which aim to remove barriers to the sharing of data across national borders.[26] But notably, one of the two countries at the heart of this volume—India—refused to sign up for Abe's Osaka initiative.

These international efforts to focus more attention on data policy should continue and should motivate both developed and developing countries to clarify the mishmash of national policies that affect how data are handled, shared, and used. International organizations have a critical role to play in showcasing how individual countries, like India and Korea, are taking steps to enable their citizens and companies to unleash the power of data. These multilateral and multinational groups, both formal and ad hoc, can push back against policies and models that would prevent that.

Open Data

The first two chapters on open data feature Rahul Matthan and Shreya Ramann on India's experience and Taewoo Nam on Korea's. Both countries are making access to government data a high priority and have legislation ensuring that government agencies share data that can be safely made public. But precisely *how* this legislation is implemented will determine the course through which many innovative and new applications of that data develop. Nam's chapter shows that in Korea, hundreds of companies are already using government data sets. In India, meanwhile, Matthan and Ramann delve into a growing debate on access to and the use of nonpersonal data, a critical ingredient for machine learning tools.

What is ultimately important is that policies for government data (and the infrastructure built to provide access to such information) offer models for access to other types of commercial and consumer data in safe, secure, and reliable ways. But unfortunately, some government data protection and data localization regulations could unintentionally severely hinder the development of these new approaches.

India's DEPA architecture is designed to improve inclusivity and allow those most in need to access online services but also have broader oversight on consent. Matthan and Ramann show that since data storage is cheap, Indian and foreign entities can amass vast volumes of it. But this data is siloed and usually only

available to those who have harvested it, while the Indian citizens to whom the data pertains have almost no say in its use. Indian data policies, they argue, aim to deal with both challenges, not just by minimizing privacy risks and potential misuse of data but by giving individuals practical means to access, control, and share their data for their own benefit. They describe regulatory and technological advances being made in India, especially around DEPA, and how such models can be used to build on data governance initiatives around the world.

For his part, Nam addresses three main issues in Korean open data policy governance: institutions, policies, and organizational capacity. In all three areas, he sees progress but finds some flaws in the country's current approach. One example is a regulatory framework that divides responsibility among diverse ministries with different approaches. This arrangement, he says, becomes even more complicated once local governments enter the mix. Public and private data cannot be easily integrated since they fall under different bureaucratic jurisdictions that functionally overlap but remain institutionally divided.

Likewise, Nam argues, Korea simply does not provide well-defined criteria for success to guide the wide variety of actors who use and leverage data. As a result, many corporate data users in the country complain about the low value of open public data while even government employees lack a substantial understanding of what data-driven administration means and why it is important for the public sector, much less the country's corporate and academic sectors.

Cross-Border Data

The next two chapters turn to cross-border data, pairing up Smriti Parsheera on India's experience with "KS" Park on Korea's. These two chapters are anchored by the pivotal roles these two countries play in the global ecosystems that require rapid and secure international sharing of confidential business data. They explore how each country has sought to manage the delicate balance between localization and internationalization.

Some proposals for data localization, often motivated by governments' desire to protect citizens' privacy or to enable law enforcement surveillance, can hinder this free flow. For example, India has, in most cases, allowed for the free movement of data across its borders, but pending domestic legislation would hamper these more open practices. Similarly, in Korea, arguments for and against localization are becoming more pronounced. The few studies that have assessed the economic impact of data localization requirements have found that limiting cross-border data flows can significantly slow GDP growth—a tricky challenge for India and Korea at a time when both countries face growing domestic and global economic headwinds.[27]

Parsheera begins with the central contradiction India faces: the country has reaped significant benefits from being digitally connected and following an open market policy, but the country is also grappling with the challenges posed by data monopolization, barriers to lawful access, and limitations on the effective enforcement of laws, rules, and regulations in the digital sphere. India aims to transition from a user to a controller in digital markets and, to this end, it has leaned on technological self-reliance combined with frequent assertions of "digital sovereignty."[28]

As in Matthan and Ramann's chapter on open data, Parsheera traces a fragmented and often contradictory Indian institutional and policy landscape. But beyond the domestic sphere, she also explores whether and how international instruments like the Budapest Convention could be useful to New Delhi. India is not a signatory to the convention, a binding multinational treaty that comprehensively addresses both cyber crimes and the gathering of electronic evidence of noncyber criminal activity.

This theme links Parsheera's chapter to Park's because he, too, notes Korea's absence from the Budapest regime. He argues that Seoul is thereby denying itself a useful pathway to pursue its interests. Indeed, Park finds much fault in Korea's localization discourse and policy. He argues that the assimilation of international arrangements and instruments could enable Korean policymakers to realize their policy goals *without* mandating such data localization. For instance, the Budapest Convention could provide an alternative to time-consuming mutual legal aid treaty processes that require law enforcement agencies to request help from their foreign counterparts. Similarly, while acknowledging concerns about citizens' privacy as an important policy goal, Park argues that the adequacy process of the European Union's General Data Protection Regulation or the certification process of the Asia-Pacific Economic Cooperation forum's Cross-Border Privacy Rules may provide the needed level of protection, no matter where the data may be stored and processed.[29]

Democratic Diversity

As the four chapters in this volume demonstrate, major Asian democracies like India and Korea are not simply following the lead of the United States and Europe on data governance. Instead, in many areas connecting to both open data and cross-border data, they are pioneering their own unique approaches, which are anchored firmly in their own consolidated democratic institutions.

The goal in this volume is to highlight these alternative models and to compare and contrast their distinctive features. Indeed, like the 2021 volume on *The Korean Way With Data*, this sequel volume demonstrates that the future will be much more complex than a putative battle between U.S.- and China-centric approaches, much less between democratic and authoritarian approaches. Much can be learned—and some things can be emulated—from the experiences of these two unique and important Asian democracies.

CHAPTER 1

India's Approach to Data Governance

RAHUL MATTHAN AND SHREYA RAMANN

India has witnessed rapid digital growth in a short time span. This has resulted in technological advances, new governance regimes, and bespoke, India-only digital policies. Taken together, these changes have come to define the Indian model of data governance. In turn, this model aims, from an Indian perspective, to empower citizens.

As the pace of government adoption of new technologies and services has picked up, public debates in India about the need to balance data rights with digital innovation have accelerated in lockstep.[30] This trend has been driven by India's rapid digital expansion and concerns that citizens unfamiliar with the potential harm that could arise from the misuse of data will suffer. Despite these concerns, India does not yet, as of August 2022, have a uniform, comprehensive data protection law, even though data has become central to most private enterprises and public initiatives.

Since data storage is cheap, Indian and foreign entities can amass, day after day, year after year, vast volumes of information on the off chance that it will be of use someday, rather than risk not having it on hand when they need it.[31] However, since these data are siloed and usually only available to those who have harvested it, little is being done to unlock the full value of the data. Worse, the Indian citizens to whom the data pertains have almost no say in its use.

Indian data policies have focused on addressing both these challenges. In addition to traditional approaches to minimizing privacy risks and the potential misuse of data, these Indian policies are also meant to provide individuals with a practical means by which they can access, control, and share their data for their own benefit.

India's approach to data governance has evolved in light of India's domestic priorities and international position. This analysis specifically describes and assesses the evolution and implementation of various regulatory and technological advances in India and how such models can be used to build on data governance initiatives around the world.

The sections below examine new initiatives and policies, evaluate the effects of India's regulatory approach on the country's domestic growth and global position, and look at the role these initiatives play in the broader data governance ecosystem worldwide.

The first section discusses India's digitization and the data boom that followed, a period that began in earnest in the 1990s. It looks at the increasing proliferation of digital services and examines how data has and will continue to affect the growth of the Indian economy. The second section looks at the existing and future legal framework for data governance in India. It covers both existing regulations as well as notable public policy proposals on personal, nonpersonal, and government data. The third section examines the technology infrastructure that the Indian government has put in place to augment legal frameworks for effective data sharing. With a focus on the implementation of the Data Empowerment Protection Architecture, this section describes India's technolegal solutions for empowering individuals to wield control over the data they generate. The fourth section concludes by weaving together themes from India's data governance strategy. It contextualizes India's proposed initiatives in relation to other global approaches to data governance. Issues such as data sovereignty and data colonialism are analyzed to assess how they affect India's standing in the global data market.

India's Data Economy

In the 1980s, India's information technology (IT) sector was focused primarily on software exports and services and was valued at only $25 million, constituting approximately 0.01 percent of India's GDP at the time—primarily because the sector was closed to the world and subject to high import tariffs.[32] Software was not a government-recognized industry, and Indian exporters were unable to convince banks to finance their activities.[33] The country's early IT industry thrived despite the government—not because of it.

By contrast, India's IT industry and related sectors currently have annual revenues of $200 billion and account for 13 percent of the country's GDP.[34] India long has been known as a global powerhouse in exporting IT services, but the country's IT sector is no longer solely dependent on exports for growth. Over the past decade, domestic demand for IT services has grown rapidly,[35] with the aggregate value of domestic demand for digital services in India outpacing the total value of exports.[36] Today, digital services are used more widely than ever in India. This change was made possible by the deep penetration of mobile internet access through all strata of Indian society—including into the country's rural hinterland. More than 750 million Indians use smartphones, or approximately 54 percent of the country's total population, allowing them to access entertainment, information, and public services on the go.[37]

In addition, over the past ten years, India has rolled out digital infrastructure on a commensurate scale, enabling residents to make rapid strides toward a paperless virtual existence, allowing them access to digital services from anywhere in the country without having to carry physical documentation or visit specific service-delivery locations. Today, more than 5.4 billion digital payments take place each month over India's Unified Payment Interface (UPI), a digital payment system that makes it easy to transfer money between bank accounts, mobile money accounts, and digital wallets.[38] These transactions range from small purchases of chai and biscuits from pushcart street vendors to substantial e-commerce payments for goods and services. The interface has also made it possible for microlevel entrepreneurs and small businesses alike to identify and take advantage of commercial opportunities that were previously unavailable to them.

A similar revolution is poised to unfold in new data services, enabled by a new digital framework in the financial services sector.[39] Other sectors (such as healthcare and education) are similarly expected to benefit from this framework.[40] Finally, work is underway to unbundle location-based digital commerce, allowing different elements across the commercial ecosystem to interact more efficiently and opening the door to greater competition between players.[41] When rolled out, this open network of digital commerce will likely reduce the dependence of consumers and smaller retailers on vertically integrated platforms in favor of a more disaggregated, decentralized approach.

Each of these projects has contributed to the widespread use of data and illustrates the importance of effective and efficient data governance. However, before getting into the details of India's data governance regime, it is necessary to first understand how the IT sector has evolved and grown to its current size and state.

India's Promotion of Information Technology

Three critical factors enabled the development of India's IT industry starting in the 1990s: the economic liberalization of 1991, industry-specific measures such as the establishment of software technology parks in 1989, and intensive government procurement of IT equipment and services. This welcoming environment encouraged several multinational companies to set up shop in India, a development that in turn sparked an IT services export boom.[42] By 2000–2001, India's total software exports grossed $6.4 billion.[43]

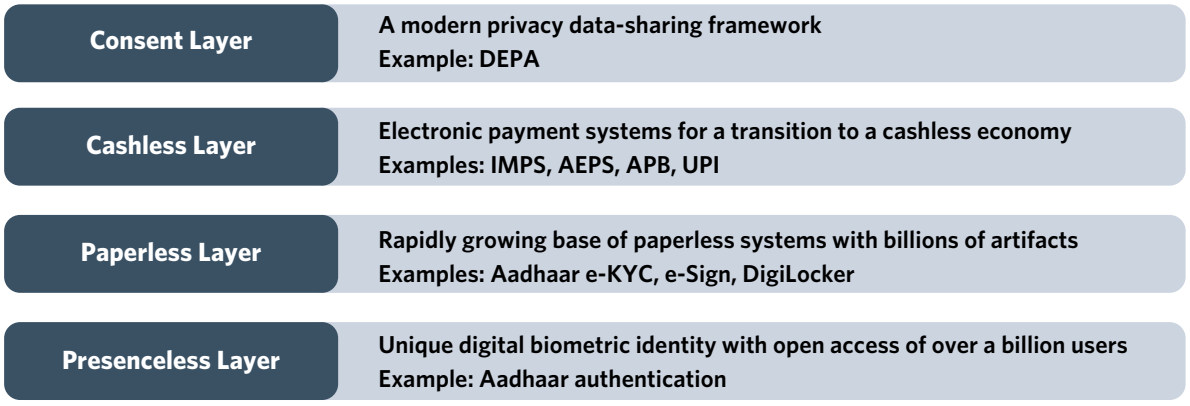
Economic reforms, liberalization, and the steadily increasing presence of foreign multinational companies in India led to several ancillary developments, including the launch of cable internet and the passage of India's first IT-related legislation.[44] In 2015, the Digital India initiative was launched.[45] This ambitious, multifaceted program aimed to transform the country's digital infrastructure into a public utility—facilitating digital governance and empowering citizens. Several additional programs have been launched under the broad umbrella of Digital India, including BharatNet (a program to provide internet access to all villages in the country), Universal Access to Mobile (a program designed to provide mobile connectivity to over 55,000 villages in India that previously lacked mobile access), and the Smart Cities Mission (a program to transform all Indian cities into smart cities).[46]

Increased digitization, the proliferation of online services aimed at Indian customers, and the use of new technologies have dramatically increased the volume of data in circulation. According to government projections, emerging technologies in India could conceivably generate as much as $1 trillion in economic value; the wealth of data in India could be harnessed to achieve the country's ambitions of becoming a $5 trillion dollar economy in overall terms by 2025.[47]

Digital Infrastructure

Over the last decade, India's digitization efforts have been greatly accelerated by the deployment of population-scale digital infrastructure. These open protocol–based frameworks, layered one on top of another, form a digital stack. At the base are foundational elements such as digital identity markers, while specific applications (including payments, consented data sharing, and unbundled commerce) are layered on top. These complementary levels of digital infrastructure are commonly referred to as India Stack (see figure 1).[48]

Figure 1. The Layers of India Stack



Sources: Tanuj Bhojwani, "The Best Way Forward for Privacy Is to Open Up Your Data," iSPIRT, August 21, 2017, https://pn.ispirt.in/the-best-way-forward-for-privacy-is-to-open-up-user-data; and India Stack, "India Stack," India Stack, https://indiastack.org.

Digital means of identification. India Stack began in 2010 with the issuance of unique identification numbers to all Indian citizens as part of the national identification program known as Aadhaar. Before the program was established, an estimated 400 million Indian citizens did not possess any form of identification.[49] As a result, citizens, particularly in the country's lower socioeconomic classes, struggled to access the government funds and subsidies to which they were entitled. This problem was exacerbated by the ease with which funds could be diverted by malicious actors. All told, depending on the program, between 10 percent and 60 percent of funds earmarked for subsidies and social welfare services fell prey to leakage or misuse, according to one study.[50]

Aadhaar was meant to provide all Indian residents with a unique identifier, making it possible to more accurately deliver services to the right people. Since the identifier was digital, it could be linked to technology-based solutions that leveraged digital verification to offer services that are presenceless, paperless, and more efficient.

The widespread adoption of Aadhaar has led to improvements in digital service delivery across India. The Indian government has issued around 1.3 billion Aadhaar cards since 2016, covering nearly 96.4 percent of the country's population.[51] This has allowed the government to make large-scale wealth transfers in an efficient manner. For instance, during the coronavirus pandemic, nearly $44 billion has been disbursed to farmers and other marginalized groups using India Stack.[52] And it is estimated that the government has saved almost $30 billion as of March 2021 by eliminating duplicate beneficiaries.[53] The adoption of Aadhaar also exposed millions of rural Indians to digital transactions and led to an uptick in digital literacy and digital penetration across the country.

Aadhaar has led to the creation of various means of authentication, including an e-authentication process in which a service provider uses an Aadhaar number to query the Aadhaar database, which is managed by the Unique Identification Authority of India. Authority officials respond to such requests by indicating if the database contains a record that matches the Aadhaar number and the details contained in the request, thus providing an accurate means of identity verification. Aadhaar's electronic know-your-customer service, which uses this authentication method, has already carried out around 75 billion identity verifications, in response to requests from the government and other institutions in finance, telecommunications, and other utilities.[54] Similarly, Aadhaar's e-sign capability allows any Aadhaar number holder to generate a legally valid, verifiable digital signature.

As the Aadhar program and related services matured, the share of India's population with a bank account jumped from 35 percent in 2011 to 80 percent in 2017.[55] The World Bank estimates that Aadhaar's know-your-customer service brought down the costs of customer onboarding for an Indian bank from $23 to just $0.15.[56] Aadhaar-based customer verification provided telecommunications companies with a huge boost in terms of customer acquisition, specifically in rural markets where there was immense untapped potential. Faster, cheaper, and simpler onboarding led one company—Reliance Jio, a late entrant to the Indian telecoms market—to decide to make Aadhar the only way for new subscribers to acquire a SIM card. Jio acquired 16 million subscribers in the first month after it opened for business and 50 million in under ninety days.[57]

Digital payments. With the penetration of mobile phone connections and bank accounts across India, policymakers needed to make bank usage cheaper and more accessible. This need prompted the design of the next layer of India Stack: UPI.[58] In simple terms, UPI is a payment markup language that runs on a central switch operated by the National Payments Corporation of India. Since all licensed banks are connected to the National Payments Corporation of India's server, payment messages can be sent to and from these entities, allowing payment transactions to take place almost instantly.

UPI is itself a three-level stack. The base layer is built and operated by the National Payments Corporation of India, and it consists of the switch that handles the routing of payment messages. The next layer involves banks and other regulated financial entities that are permitted under law to hold user funds and pay and receive amounts into these accounts. The third and top layer is made up of payment apps operated by lightly regulated fintech players that create customer interfaces that allow ordinary users to access the payment ecosystem. Given the fundamental interoperability of these protocols, every participant in the payment stack can interact with every other participant using the same universal set of application programming interfaces (APIs). As a result, the Indian payment ecosystem has avoided having to laboriously establish one-to-one relationships between banks to make it possible for customers to transfer money to each other.

Another UPI innovation is its use of a virtual payment address (VPA), a unique identifier that maps a given user's bank account to an easily memorized string of names, letters, and numbers that can be shared for the purpose of receiving payments. While this method offers the advantages of privacy and security (because knowledge of a VPA offers no information whatsoever about the associated bank details), since the VPA is ubiquitous throughout the ecosystem, the VPA is agnostic to payment apps, allowing money to be exchanged even between users on different payment apps.

In June 2022, an estimated 5.9 billion transactions, amounting to about $127 billion, were conducted using UPI, and it has been a recognized success both in India and abroad.[59] A wide range of internet and mobile offerings have been integrated into the UPI ecosystem, with foreign players such as Amazon, Google, Meta, and Walmart relying on it in India.[60] Countries like the United States have also been considering adopting UPI features within their own domestic payment systems.[61] UPI has emerged as a leading homegrown payment system with the potential to give India self-sufficient alternatives to reliance on global payment solutions.

Data sharing. Having built widely trusted identification and payments systems, India consequently began to generate vast amounts of transaction data. The next logical step was to use this data for empowering citizens eager to use e-commerce and e-government services, particularly those who had no other means of accessing the formal financial system.

The third layer of India Stack, called the Data Empowerment and Protection Architecture (DEPA), was designed to facilitate consented data sharing. Unlike previous layers that were predominantly technological, DEPA is, by its design, a technolegal architecture that individuals can use to exercise greater autonomy over how their personal data are used. It offers technological tools for people to invoke the rights made available to them under applicable privacy laws. Framed differently, it is a technological system that ensures that all transfers of a person's data from one data fiduciary to another take place through an encrypted digital workflow that is only triggered after that person's consent has been electronically obtained.

DEPA has already been rolled out in the financial services sector, and work is underway to implement it in the healthcare system. It is not hard to envision how this framework can be applied across a range of sectors such as education, telecommunications, and more. The data governance principles inherent in the technological design of the DEPA framework are examined in more detail below.

India's Need for Data Governance

With the launch of Digital India and the India Stack, the prevalence of smartphones in rural India grew from 9 percent to 25 percent by 2018, the number of Indians who use social media jumped from 142 million in 2015 to 326 million by that same year, and between 2015 and 2018 average data usage each month increased by 129 percent (assuming a compound annual growth rate).[62] The direct impact of the aggressive digitization of the Indian economy has been the unprecedented volumes of data that have been and continue to be generated. India's online population is expected to increase by nearly 45 percent in the next few years, growing from approximately 622 million in 2020 to 900 million in 2025.[63] The amount of wireless data Indian consumers use increased by leaps and bounds to reach over 30,000 petabytes in the first quarter of 2021–2022. At the same time, the average consumer went from using 1.2 gigabytes of wireless data in 2017–2018 per month to a staggering 14.1 gigabytes in 2021–2022.[64] Monthly data consumption is also expected to climb to up to 50 gigabytes per smartphone by 2027.[65]

India is now digitizing faster than most other economies, creating a rapidly growing consumer base that is being targeted by both domestic and foreign companies. It goes without saying that, without an appropriate system of governance, the benefits that are being derived from all this data might not be enjoyed by all Indian citizens. India is looking to bridge the regulatory gap between burgeoning data creation and the need to regulate and leverage available data. In doing so, India has developed frameworks for both data protection and data sharing, measures that aim to further both government and private-sector use of data for socioeconomic benefits.

Legal Frameworks for Data Governance in India

While there are several types of data in circulation and various issues pertaining to the governance of each kind, this analysis exclusively deals with data types that the Indian government is actively looking to regulate, such as personal data generated from individuals and nonpersonal data, which in some cases may also be derived from personal data but also includes data with no relationship to individuals. This research does not examine how other types of data—including scientific data, commercial data, and the like—are shared, though these kinds of data are equally important to broader discourse on data governance. Indian data governance practices will primarily be analyzed in terms of data sharing between government entities, businesses, communities, and ordinary people for both public-good and business purposes.

It is also important to set out the different stakeholders in the Indian data ecosystem so as to better understand the interplay between them. The priority of the Indian government is to use digital technologies for domestic development, leveraging data for the benefit of its citizens and for their protection. The private sector, which is largely focused on commercial gain, used to view data governance as a hindrance, but in more recent times companies have come to appreciate that customers view good data governance practices positively. Finally, individual citizens and the communities that they are a part of have an interest in ensuring that they can exercise meaningful control over their data to protect themselves against potential harms.

Around the world, data governance is implemented by regulating the collection and use of personal data. In most countries, such regulations have taken the form of data protection legislation that sets out what can and cannot be done with personal data and strives to ensure that citizens have a greater say over how their data are used. In recent times, other aspects of data governance have also come into focus. The European Union's Digital Strategy, for example, attempts to regulate digital markets in goods and services to promote greater competition while facilitating the creation of so-called data spaces within which data can be shared.[66] Similar efforts are underway to regulate the use of data for developing artificial intelligence systems and to mitigate the effects of such systems on personal privacy.[67]

Though India has made considerable strides in digitizing its economy, Indian legal frameworks have not kept pace with this rapid growth. India does not yet have a comprehensive legal framework for data governance. A draft data protection law had been introduced before the parliament, but it was recently withdrawn.[68] It is likely that a simplified and more comprehensive version of the draft bill will be introduced, but the timeline is unclear.

Delays in establishing a comprehensive legal framework for data governance could play to India's advantage if it can learn from the experience of other countries and use that knowledge to implement a modern framework for data governance. This could include some of the proposals being discussed in Europe as well as other novel solutions aimed at addressing these issues. India's DEPA framework (described in more detail in the next section) is one such novel solution: this technolegal governance regime embeds data protection principles into a technology stack.

In the meantime, this section will discuss the legal frameworks that India has put in place for data governance as well as the proposals for new legal frameworks that are being considered. The subsequent section will then examine the technological frameworks that have already been implemented for data governance in India.

Data Governance in India

At present, India regulates personal data through the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which serve as a basic framework for regulating sensitive personal data.[69] These rules do not provide a comprehensive framework for data protection along the lines of most data protection laws in other jurisdictions. (They do not, for instance, regulate children's data rights or cross-border data transfers, nor have they even established a data protection regulator.) Instead, these rules are limited primarily to the collection, possessing, storage, handling, retention, transfer, and disclosure of sensitive personal data by corporations through the introduction of a consent requirement for all such activities. The law also prescribes certain "security practices and procedures" for the handling of sensitive data.[70]

Although these rules came into force more than a decade ago, delays and insufficient administrative and adjudicatory mechanisms have plagued its implementation.[71] Since 2011, there has been little or no regulating carried out under its provisions. Companies comply with its provisions but have received little or no guidance on how to handle the many ambiguities that have arisen.

Indian citizens and civil society, however, have grown increasingly aware of the harms that are inherent in the collection, generation, and processing of personal data. In 2018, a landmark Supreme Court judgment, which upheld the use of India's Aadhaar digital identification numbers, had to address concerns around government profiling and surveillance. The Supreme Court in another judgment in 2017 had held that the right to privacy is a fundamental right that—while not specified in the Indian Constitution—is derived from the right to life and personal liberty.[72] These rulings focused public attention on the rights of individuals to have autonomy over what is done with their data.

India's approach to data governance is proceeding along three different tracks. First is the regulating of personal data in ways that draw heavily on the principles set out under the EU's General Data Protection Regulation (GDPR) as well as other international regulations on personally identifiable information. Second, India is in the process of establishing a nonpersonal data framework—a path down which no other country has yet embarked. The broad contours of this policy can be gleaned from draft reports released by a Committee of Experts known as the Gopalakrishnan Committee.[73] The third aspect of this work has to do with the governance of government data, which is covered under the National Data Sharing and Accessibility Policy.

Personal Data

While the Supreme Court was still considering the constitutionality of the Aadhaar program, the Indian government established a committee, chaired by retired justice B.N. Srikrishna, to look into the establishment of a personal data protection law for the country. The committee issued its report in 2018 along with draft legislation.[74] In December 2019, the Ministry of Electronics and Information Technology introduced in the Indian parliament a slightly revised version of the legislation called the Personal Data Protection Bill, 2019.[75] The bill was referred to a joint parliamentary committee for further consideration. After consulting with various stakeholders, the joint parliamentary committee published a December 2021 report, along with yet another draft bill.[76] The revised law was called the Data Protection Bill, 2021 (DP Bill). While the bill has now been withdrawn, its provisions signaled the government's approach and likely policy shifts with respect to personal data. The key features of the bill are highlighted below.

The DP Bill defined personal data as information "about or relating to a natural person who is directly or indirectly identifiable" (by "natural person," the bill meant a human being as opposed to a nonhuman juridical person such as a corporation or a government agency).[77] Such data specifically is information pertaining to a feature of identity (virtual or physical) or a combination of such features, including "inferences drawn from such data for the purpose of profiling."[78] This definition is largely in line with those of similar laws elsewhere, like the EU's GDPR.[79] The DP Bill also defined sensitive personal data, a separate class of data subject to enhanced compliance thresholds. Sensitive personal data include financial data, healthcare data, official identifiers (including government-issued identifiers such as social security numbers or Aadhaar numbers), information on gender identity and sexual orientation, biometric data, genetic data, caste or tribe affiliations, religious or political beliefs or affiliations, and any other category of information so designated in the future by the relevant authorities.[80]

As for the entities involved in data processing, the DP Bill defined a data fiduciary along similar lines as GDPR defines a data controller.[81] The DP Bill referred to the individual whose personal data is being gathered as the "data principal," a term equivalent to the concept of a "data subject" in GDPR.[82] Consent remains the primary grounds for processing personal data.[83] However, similar to other privacy legislation, the DP Bill also specified a few nonconsensual grounds for data processing.[84] In line with both the Indian government's aim of ensuring individual autonomy over data as well as global norms, data principals have been accorded various rights with respect to their data under the control of a data fiduciary; these provisions include the rights to access, erasure, correction, and portability, as well as the right to be forgotten.[85]

The DP Bill also introduced the concept of consent managers—a new category of data fiduciaries to operationalize consented data flows.[86] Data principals were meant to provide consent through these consent managers to share information with various data fiduciaries.[87] This construct would support the DEPA framework, as discussed in the third section.

The DP Bill aimed to create a Data Protection Authority to govern implementation and enforcement of the law. In theory, the Data Protection Authority could designate certain entities as "significant data fiduciaries."[88] Such determinations were to be made based on criteria like how much personal data has been processed, how sensitive it is, the scale of the fiduciary's annual turnover, the "risk of harm" from data processing, the employment of new technologies, or whether the entity processes children's data or provides services to minors.[89] Social media platforms that have more than a specified number of users or ones whose actions "are likely to have a significant impact on electoral democracy, state security, public order, or India's sovereignty" also may have been designated as significant.[90] Significant data fiduciaries would have been subject to greater compliance obligations including the need to undertake mandatory data protection impact assessments as well as record keeping and audit requirements.[91] They also must appoint a data protection officer.[92] India is among the first nations to press heightened obligations on a certain class of data fiduciaries, with parallels only now appearing in regulations such as the EU's Data Governance Act.[93]

The DP Bill deviated from other countries' data protection legislation in certain key aspects. Prominent among these is the fact that, under the DP Bill, a child was defined as a data principal under eighteen years of age.[94] This is a higher age cutoff than has been prescribed in most other jurisdictions.[95] Data fiduciaries have an obligation to confirm the age of minors and to get parents' consent to process their data.[96]

The DP Bill did not subject personal data to any transfer restrictions. Its terms "allow transfer of sensitive personal data, for the purpose of processing and with the explicit consent of the data principal, to any countries with certain safeguards."[97] The DP Bill also empowered the central government to designate certain types of personal data as "critical personal data," which could only be processed in India and could only be transferred outside the country for limited purposes.[98] What constitutes critical personal data still remains undefined.

The DP Bill also allowed for compensation to be paid to data principals for harm caused to them by a data fiduciary because of a violation of the bill's provisions.[99] The definition of harm under the DP Bill was very broad and extended to all types of evaluative decisions regardless of human involvement.[100] Notably, the concept of harm is defined more specifically in data governance laws in other jurisdictions such as the EU's GDPR and the draft of the United Kingdom's Online Safety Bill. The definition of "content that is harmful" in the draft UK bill is very specific regarding the parameters within which harm must be assessed. The law provides definitions and further context on the scope of what harm means and key definitions, including terms such as "reasonable grounds" and "material risk," as well as factors to take into account when making such an assessment.[101]

Once India passes a data protection law, there will likely be a transition period during which data fiduciaries will have to prepare themselves for the new regulatory regime. This is also when the Data Protection Authority will be established and tasked with setting up the administrative framework for implementing the new law. This task would include issuing codes of practice establishing, through subordinate legislation, many of the substantive and procedural details required to bring the law into force.

Several provisions of the DP Bill prompted a strong response from governments and businesses around the world. The U.S. government, for instance, sees the Indian government's push for data localization as a significant barrier to digital trade between the two countries.[102] U.S. officials have suggested that the requirement would result in increased costs for businesses that presently store and process data outside India and in particular would act as a market access barrier for small foreign firms.[103]

Industry bodies such as the U.S.-India Business Council, the U.S.-India Strategic Partnership Forum, the Information Technology Industry Council, BusinessEurope, and the Japan Electronics and Information Technology Industries Association, as well as major technology players that provide services in India such as Microsoft, Apple, Amazon, Google, and Dell have raised concerns (in addition to the localization issue) about provisions such as the inclusion of nonpersonal data in the bill and mandatory hardware certifications.[104] They argue that such provisions are not in line with global best practices for data protection and that such stipulations would create disincentives for innovation in India by reducing operational efficacies and lessening the ease of doing business.

Nonpersonal Data

Various public and private entities have also accumulated vast, proprietary sets of nonpersonal data that they can leverage to their competitive advantage. If such nonpersonal data could be liberated from the exclusive control of their current holders, it is believed that this information could be redeployed for the public good.

The need to regulate nonpersonal data was first expressed in the report by the Srikrishna Committee on personal data protection. The early draft of the law also referred, albeit by exclusion, to the concept of nonpersonal data. In the fall of 2019, the Ministry of Electronics and Information Technology convened

the Gopalakrishnan Committee to brainstorm how India should govern nonpersonal data. The committee was tasked with studying various issues related to nonpersonal data and making specific recommendations on how the central government should regulate nonpersonal data.

The latest draft of the committee's report was released for public consultation in November 2020.[105] While the committee's final findings are not yet public, the latest draft report suggests that the governance framework for nonpersonal data in India will cover the following ground.

The Gopalakrishnan Committee defined nonpersonal data as data that never related to an individual (such as weather conditions or data generated from public infrastructure, to cite a few examples) and information that was once personal data and subsequently was anonymized in such a way that it cannot be used to identify an individual (such as anonymized healthcare records of patients). Nonpersonal data only refers to these two categories of data. The committee's report classified entities (whether government bodies or private organizations) that collect, process, store, or manage data as data businesses. These entities hold nonpersonal data that the proposed governance framework seeks to unlock for public benefit.

The report also gave communities rights over data that are relevant to them. A community is defined in the report as any group of persons bound by common social or economic ties, territorial parameters, or another interest or purpose. The Gopalakrishnan Committee expressed the belief that communities should be allowed to benefit from data that pertains to them and allowed to protect themselves from any harms that could arise when data businesses process their data.

The Gopalakrishnan Committee recommended the establishment of a separate Nonpersonal Data Authority. This authority would be required to work closely with the Data Protection Authority that the DP Bill sought to establish. While this suggestion indicates that the Gopalakrishnan Committee supports a framework for the regulation of nonpersonal data that "is separate and distinct from [that for] personal data," the DP Bill appeared to also regulate nonpersonal data.[106] Two provisions in the DP Bill mentioned nonpersonal data: clauses on breaches involving nonpersonal data and those on the obligation of data fiduciaries to provide the central government with nonpersonal data for the "targeted delivery of services" or "evidence-based policy making."[107]

To protect the rights of communities in relation to their nonpersonal data, the Gopalakrishnan Committee recommended the creation of data trustees (either government entities or private nonprofit organizations) for this purpose. After all, "data trustees have a duty of care" to ensure that nonpersonal data are used only in the interests of these communities.[108] To effectively protect communities' data rights and ensure public benefits are derived from nonpersonal data, the report recommended that data trustees become the repositories for high-value data sets created from community data.

One of the report's core recommendations was the creation of high-value data sets. All data businesses will be required to submit metadata pertaining to all the nonpersonal data under their control. This metadata will be stored in a single metadata directory and managed by the Nonpersonal Data Authority.

The directory will be made available for anyone to access, allowing data trustees to identify opportunities in which such data could be used for public good. Data trustees will have the right to request access to relevant data subsets to create a high-value data set. The relevant data business must provide such data by a specified date.

Crucially, high-value data sets could only be created with the approval of the Nonpersonal Data Authority, a body set up for the supervision of nonpersonal data sharing. The authority would approve applications based on their projected impact on the public interest, the data trustee's capacity to undertake its obligations, adequate buy-in from the relevant community, and public consultation. This purpose-driven approach to data sharing focuses heavily on the manner in which nonpersonal data can be used and predicates data sharing on the basis of advancing the public good. The report clarified what constitutes a high-value data set that serves the public good, with examples of such purposes including research and education, healthcare, agriculture, and poverty alleviation, to name a few. Parallels may be drawn with the United States' Demand-Driven Open Data model, which regulates data-sharing requests based on specific use cases.[109] This demonstrates the government's intent to create a framework that focuses not only on protection from harm but also on the societal benefits that can arise from the sharing of nonpersonal data in a regulated ecosystem.

As for data that was once personal but has since been anonymized, the report recognized the rights of the original data principals. The report recommended that, when the personal data are collected, data principals decide whether to provide consent for a data business to anonymize their data. Such consent should also be revocable.

With regard to nonpersonal data that is derived from personal data, the report suggested that such data would "inherit the sensitivity of the underlying personal data" for the purposes of complying with localization requirements.[110] For example, based on the DP Bill, a copy of nonpersonal data derived from sensitive personal data has to be kept in India.[111]

India's nonpersonal data governance framework is novel. While the principles enshrined in the DP Bill protected personal data from misuse by data fiduciaries, the framework for nonpersonal data was designed to free up data that is not personally identifiable so that it can be used for the sake of wider societal benefits. Whereas on the one hand the data protection framework would lock down data that ought to be kept private, the nonpersonal data framework would unlock data that can be used for public good from the confines of the data silos in which they are stored.

Concerns have been raised about the imposition of mandatory data sharing. At the same time, businesses have questioned whether such a regime would be able to address skewed market powers favoring large technology companies who hold vast amounts of nonpersonal data.[112] Some have argued that data-sharing requirements of this kind have the potential to obstruct innovation, thereby hampering India's digital growth.

Government Data

Even though nonpersonal data held in government hands is expressly accounted for in the proposals of the Gopalakrishnan Committee, the Indian government has separately created a policy to deal with the sharing of such data for the public good. The National Data Sharing and Access Policy makes disparate government data assets available for the public to access.[113]

The policy applies to all nonpersonal and nonsensitive data generated using public funds across all levels and departments of the government and its authorized agencies. The data that must be provided under this policy include all digital, analogue, machine- and human-readable formats, and suitable payment structures have also been set up to incentivize data sharing. The government has taken a technolegal approach to this task by developing the Open Government Data Platform on which data shared under the National Data Sharing and Access Policy are made publicly available.

Since the launch of the Open Government Data Platform in 2012, several other open data platforms have been launched. As Sam Neufeld has pointed out, examples include the India Urban Data Exchange of the Ministry of Housing and Urban Affairs (an open-source data exchange for citywide data among various stakeholders), Open Budgets India created by the Centre for Budget and Governance Accountability (which includes data on central and state budgetary allocations and spending), and the proposed National Data and Analytics Platform by NITI Aayog, a platform that aims to improve the user experience on data retrieval by standardizing data across government sources for improved research, innovation, and public consumption.[114]

While the Open Government Data Platform offers more information and data to users, as well as functionalities for social media, data visualization, and data suggestion, there are many opportunities to strengthen its utility. For instance, standardizing data-sharing and release processes, anonymization and deidentification processes, metadata quality, licensing structures, and the pricing and valuation criteria for data sets will encourage more data-sharing efforts by Indian government departments.

To this end, the Indian government has introduced a revised draft of the India Data Accessibility and Use Policy and a draft of the National Data Governance Framework Policy,[115] which aim to build upon the National Data Sharing and Access Policy and increase access to government data by leveraging emerging technologies. The draft of the National Data Governance Framework Policy focuses on the sharing of nonpersonal data collected by the government from Indian citizens and residents through the India Datasets Program. This policy introduces a new framework for the governance of citizens' data that will include the creation of the Indian Data Management Office to establish a large repository of Indian data sets and set standards for storing and collecting such data sets.

The Indian Data Management Office expects private entities to contribute to the data sets as a part of this program. This office will be responsible for ensuring that data principals retain ownership over all such data. Any requests by third parties for nonpersonal or anonymized data sets will be vetted by the

Indian Data Management Office before the data are dispersed. The office can receive and vet requests for these data sets from researchers, startups, and private companies, and it has the ability to limit the number and range of data requests from an entity. These policies are in the drafting stage and are awaiting public comments.

Technological Frameworks for Data Governance in India

The last section discussed the legal frameworks that are being developed in India for data governance. These frameworks are already novel in that they not only look to regulate the processing of personal data but also seek to unlock nonpersonal data from isolated silos to advance the public good. However, the Indian approach to data governance has one additional nuance—namely, DEPA. This is a technolegal framework for consented data sharing between data fiduciaries, as articulated in the DP Bill.[116] The framework would embed legal principles in technological infrastructure developed for the DEPA, offering novel solutions to data regulation challenges that have vexed countries around the world.

What Is DEPA?

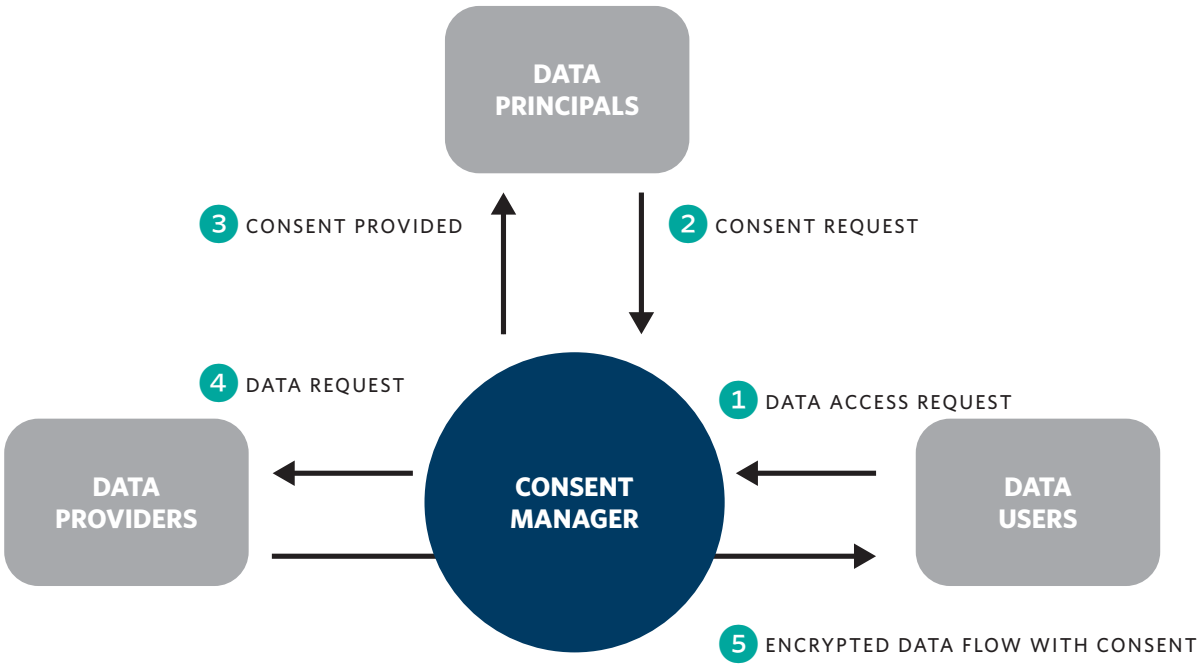
Even though privacy laws recognize the rights that data principals have over their data, they often lack a means for principals to exercise meaningful control over their personal data. For instance, citizens trying to use financial products and services that require evidence of creditworthiness often suffer if they are unable to effectively access their own data. The process often involves physically gathering one's own data from financial institutions, a cumbersome task that involves physical printouts, notarization, and manual submission. Digital mechanisms to implement data portability are hamstrung by the existence of multiple differing data storage formats and a fundamental lack of standardization across the ecosystem.

To address this, India is seeking to implement DEPA, a technolegal solution that uses an electronic, consent-based framework to put data principals at the center of data sharing in certain sectors, including finance and healthcare. DEPA gives individuals greater agency over how their personal data are transferred, helping them use data in ways that will ultimately empower them. Central to the privacy-enhancing nature of the framework is its use of institutional intermediaries to facilitate consent (called consent managers). This makes it possible to disaggregate the consent flows from the data flows: data providers are primarily responsible for data and consent managers are primarily responsible for consent. This arrangement enables a double-blind data-sharing environment that maximally protects the private information of data principals.

In figure 2 below, entities requesting access to data (known as data users) have been arrayed on the right while the entities that have the data that the data users require (data providers) have been arrayed on the left. In the middle is the consent manager, and right on top is the data principal.

This model has been fully implemented in India's financial sector under the Reserve Bank of India's Nonbanking Financial Company Account Aggregator Directions, 2016.[117] It implements consented data sharing between different parties in the financial ecosystem including banks, insurance companies, pension funds, and all entities regulated by the country's securities regulator. Specific financial entities have been permitted to register as account aggregators, which play the role of consent managers and oversee financial data flows between service providers in the sector.

Figure 2: The Role of Consent Managers



Source: Authors' visualization.

First, any data principal who wishes to transfer their financial data between various fiduciaries so as to use various financial services must first enroll with an account aggregator (or consent manager). At this stage, the data principal provides the consent manager with a list of all the financial service providers (that is to say, data providers—including insurers, banks, brokers, credit rating agencies, and others) with whom the person has an account. The consent manager then creates links to all these data providers; this way, when a data transfer request is received, it has an approved list of data providers from which data can be requested. At no stage does the consent manager have any visibility into the contents of these accounts or into any of the personal or financial data of the data principal. After this initial preparatory work, the data principal is ready to approve financial data transfers using the DEPA infrastructure.

To initiate a data transfer, financial institutions that require customer data to provide services can direct such a request (step 1) to the consent manager. The request is made using a digital consent artefact, a "machine-readable document" that records the details and specifications of consent provided alongside a data-sharing request.[118] A digital consent artefact requires the data user to provide details on the information sought, the purpose for the request, the duration for which the information will be retained, and the financial institution seeking this information. The consent manager then sends this request to the data principal (step 2) and, if the data principal consents to the data transfer (step 3), sends the digitally signed request for data to the data provider (step 4). Having verified that the data transfer request was approved by the data principal, the data provider then transfers the required financial data in accordance with the request. The data are encrypted and transferred from the data provider to the data user through the consent manager (step 5).

As of August 2022, six nonbanking financial companies have been given a license to operate as authorized aggregators, and five of them have launched client-facing mobile applications.[119] At this time, the authorized aggregator ecosystem has successfully fulfilled more than 1 million consent requests.[120]

Privacy by Design

Many data protection laws around the world are broadly aligned around a common set of what are known as privacy by design principles.[121] DEPA implements a technological framework that supports and complements each of these privacy principles.

Notice and consent. Encoded in the electronic consent requests are all the notice requirements that most international privacy laws require. Consent is specifically collected for each data transfer request. In this way, DEPA offers data principals the opportunity to provide more meaningful consent than is otherwise possible.

Purpose limitation. Data users are required to specify how they intend to use the data before it is collected and used. DEPA enables more effective purpose limitation since the data principal is notified of each data transfer request.

Data minimization. DEPA allows the purpose to be narrowly defined since it must be stated proximate to the time of the data transfer request.

Retention limitation. Each data transfer request under DEPA includes how long the personal data will be kept. Since the data are transferred only for as long as it is needed for processing and after that must either be transferred back or destroyed, data users are not permitted to retain such data any longer than specified.

Data integrity and confidentiality. Since all data transfers under DEPA are encrypted end-to-end, data confidentiality is built into the system's design. DEPA was designed with privacy at its core. Consent managers are, as a matter of design, data blind and have no visibility into the contents of encrypted data

packages. Since data requests are not made directly from data users to data providers, data principals' privacy is protected vis-à-vis data users. Since consent managers are data blind, data principals' privacy is also protected vis-à-vis consent managers.

The Digital Consent Artefact

Consent is processed using the digital consent artefact. The electronic consent artefact used by DEPA implements the so-called ORGANS principles: open, revocable, granular, auditable, notice, and secure (see below).

- **Open:** the consent standard is designed to operate as an open standard ensuring that all institutions have the same interoperable approach to consent;
- **Revocable:** the consent is designed to be revocable at any point in time by the data principal who provided it;
- **Granular:** consent needs to be provided in each instance and must specify what data has been requested, how long it will be retained, and who will process it;
- **Auditable:** records of all consents provided by a data principal can be retained in machine-readable logs;
- **Notice:** data principals will be provided notice of how their data will be used, the parties that will process it, and the duration for which it will be retained; and
- **Secure:** the digital consent artefact is secure by design.

When a data transfer request is made, verification by the consent manager happens only against the details contained in the consent artefact, and data users must store the data according to the consent artefact's specifications.

When DEPA's digital consent workflow is combined with the right to data portability provided to data principals under the DP Bill (or a similar piece of legislation) and applied to the healthcare and finance sectors, this development will help formalize the DEPA framework within and across all these sectors.

For instance, a core component of India's healthcare digitization mission is the creation of digitized healthcare records that citizens can easily access and transfer to different service providers in the healthcare ecosystem, per their requirements. Citizens may need to transfer healthcare records from a hospital or clinic to their health insurance provider to file an insurance claim. Rather than reproducing their healthcare records or status, they can use DEPA to transfer their health records from the hospital (data

provider) to the insurer (data user) through a data intermediary designed specifically for the healthcare sector (consent manager) to oversee the transfer of this sensitive medical data. This arrangement would go a long way toward facilitating constructive public health outcomes. The DEPA framework is being used for this purpose, ensuring the privacy and authenticity of healthcare data transfers.[122]

Another technolegal framework for data sharing is the Open Government Data Platform. The platform hosts all government data published under the National Data Sharing and Access Policy and enables public access to and the downloading of such data. Developed using open source stack, the platform contains multiple modules and APIs, including a module for data management that hosts data catalogues by various government agencies and a module for visitor relationship management, which collates and disseminates viewer feedback on various data catalogues.

Several state governments have launched their own open data portals using the Open Government Data Platform's software as a service model, including the Open Government Data Portal by the state government of Sikkim and a portal by the Surat Municipal Corporation.[123] India's Open Government Data Platform is also packaged as a product and has been "made available in open source" for countries around the globe to implement.[124]

India's Approach to Data Governance

India's data governance regime has been shaped by the country's historical development, the value evident from increased data generation, civil society activism, and digital innovation outside of the country. While India's efforts at developing a data governance regime have been influenced by global regulations such as GDPR and the Asia-Pacific Economic Cooperation's Privacy Framework, the Indian government is, at the same time, looking to chart its own path in certain respects.[125]

The passage of a new personal data protection law has assumed paramount importance. However, the protections proposed in the law additionally focus on improving data accessibility and availability, in contrast to GDPR, which is first and foremost about protecting individual privacy rights. These Indian policy frameworks on personal and nonpersonal data indicate that, while data protection is essential, data sharing and data empowerment are the most important drivers of India's strategy on data governance.[126]

The Indian approach is also distinct from other global models due to the tools and mechanisms that support the proposed regulatory framework. The development of unique digital infrastructure projects such as the India Stack provides policymakers with the resources to implement unique citizen-centric solutions, while also offering important lessons to other nations.

The Technolegal Approach

A central feature of India's data governance approach is its use of homegrown technolegal mechanisms. These regulatory frameworks and technical systems are used to implement policy objectives through technology design. India views frameworks like DEPA as necessary for data empowerment. Indian officials have even gone so far as to compare DEPA's design to the development of Transmission Control Protocol/Internet Protocol for online communication and GPS for navigation.[127] This approach is similar to that described by the U.S. legal scholar Lawrence Lessig, who has suggested that software and systems often can shape behavior and the adoption of technology at least as effectively as regulations.[128]

Technolegal solutions such as DEPA, the Nonpersonal Data Framework, and the Open Government Platform make it possible to develop markets for data transactions, creating interoperable grids for seamless data sharing. The role of technology in these mechanisms is clear. Entities that act as intermediaries in such ecosystems (the consent managers within DEPA and data trustees for nonpersonal data) should ideally be entities with considerable technology-related organizational capacity.[129]

India's Push for Data Sovereignty

The development of these frameworks has been driven, in part, by the objectives of India's digital policies. The Indian government is working to ensure that Indian data are domestically controlled and leveraged so that Indian citizens' data serve national interests before those of foreign players.[130] The government, supported by Indian industries, has moved to promote the domestic use of data while guarding against the threat of data imperialism (or data colonialism) by foreign technology companies.

This focus on data sovereignty stems from multiple policy goals. Given India's increasing focus on the value of data as a tool for economic growth, there has been a push to retain data in the country so that such information can be used by domestic players. Similarly, there have been efforts to more aggressively regulate the activities of foreign technology players who have access to Indian data. Concerns that foreign tech giants have too much control over India's technology landscape have led to further concerns about the misuse of and lack of access to Indian data that are stored overseas. In addition, concerns have proliferated about how market dominance leads to imbalances in bargaining power between foreign tech giants on the one hand and Indian citizens, businesses, and the government on the other.[131]

This thinking is evident in recent measures on data governance that the Indian government has introduced, the most significant of which is a cross-governmental push for data localization. Through sector-specific regulations in the banking, insurance, and telecom sectors; the DP Bill; and the nonpersonal data framework, the Indian government has made it clear that certain types of data will have to be stored within the country to enable domestic access. The primary policy goals in support of these measures are the need to overcome barriers faced by law enforcement personnel who struggle to access Indian data stored in other jurisdictions and the importance of ensuring the accessibility of Indian data to domestic players so that the relevant economic and social benefits can be tapped into.[132]

The nonpersonal data framework explicitly calls out this principle of data sovereignty, recognizing it as a key to unlocking economic benefits from nonpersonal data for India and its citizens, communities, and organizations. Other policy documents "reconceptualize the notion of community data as 'societal commons' or a 'national resource,' where the undefined 'community' has rights to access data but the government" retains ultimate control over the use of such data to advance the public welfare.[133] The requirement for mandatory data sharing under the proposed nonpersonal data framework is also indicative of the government's push to democratize the use of data and to disrupt the monopolization of data in the hands of a few companies.

That said, questions have been raised as to whether India's decision to exert its right to data sovereignty by extending its data governance framework to also cover nonpersonal data is going too far. Nonpersonal data covers a broad swathe of information that would otherwise have been left untouched, potentially affecting the rights of commercial enterprises to their trade secrets and confidential business practices. There is also the question of how exactly nonpersonal data will be distinguished from personal data given the numerous examples of how, even after it has been anonymized, personal information has been reidentified.[134] The still-awaited final report of the Gopalakrishnan Committee might hold answers to these questions.

India's Approach in a Global Context

India's approach to data governance should also be viewed within a larger global context. Many nations are starting to weigh in on the question of regulating cross-border data flows. Japan has advocated for the free flow of data across borders, a position formalized in its leadership on the Osaka Declaration on Digital Economy in 2019.[135] The United States has adopted a laissez-faire approach that supports the unrestricted flow of data across borders. The United States does not have all-purpose federal legislation on data protection for either personal or nonpersonal data. In contrast, Europe has codified data governance through various directives and acts of legislation, which individual countries have implemented.[136] Europeans have taken a human rights–based approach to data sharing by permitting cross-border sharing under specific circumstances to countries that meet the EU's requirements.

China has a radically different approach to data governance. Its cyber sovereignty approach involves the use of advanced technologies for the aggressive enforcement of sovereignty, data localization requirements, and strict monitoring of domestic data.[137] This approach has been adopted to varying degrees by other nations such as Russia and Egypt.[138]

In contrast, India declined to sign the Osaka Declaration promoted by Japan at the 2019 Group of 20 (G20) summit out of concerns that the negotiations conflicted with its policy priority for data localization.[139] This has made it clear that economic, national security, and developmental ramifications can no longer be separated from domestic or international data governance efforts.[140]

There are lessons to be learned from the data colonization of African nations that suffered from the absence of robust data protection policies. Indigenous technology development on the African continent is heavily influenced by large technology giants from the United States and China.[141] Several African nations, such as Nigeria and Rwanda, are now considering localization regulations of their own to counteract these effects.[142]

India is charting a new path for data governance. Given the size of the country's population (a significant share of which has yet to come online), its growing technological prowess, and its novel governance solutions, India can play a decisive role in shaping global data governance.

The authors' views represent their own independent analysis and should not be understood as representing the official policy of any government.

CHAPTER 2

Open Data Policy in Korea

TAEWOO NAM

Having taken office in May 2022, South Korean President Yoon Suk-yeol and his administration are well-positioned to define new and far-reaching policies on open data. But to do so, his team will need to build on the sometimes-uneven efforts of his two predecessors, former presidents Park Geun-hye and Moon Jae-in. Despite substantial differences in their ideological orientations, the conservative Park and the progressive Moon both championed the concept of "open government," which includes open data and freedom of information.[143]

For South Korea (hereafter Korea), open government is focused particularly on how open data can spur a digital transformation and unleash the technologies of the Fourth Industrial Revolution. While Korea's emphasis on and commitment to digital technology is well-known, how these efforts could be translated into more extensive cross-organizational interactions and even collaborative forms of governance has gained less attention. The good news is that successive Korean governments have developed a shared aspirational vision. The next challenge will be to address critical managerial and institutional needs, both of which are necessary for successful open government initiatives.

Since open data is the foundation of open government, this analysis discusses key issues related to Korean open data policy. In Korea, the term "public data" is sometimes used interchangeably with open data in English translations. It is believed that open data starts with releasing and sharing government-held data. When it comes to data in Korea's case, the term "public" is often confused with "open" because open data actually means open public data (given restrictions on opening private data).

Technology can lead to further openness, but only if organizational and cultural barriers are removed. Even with well-funded public initiatives, strong executive leadership, and long-term political commitments, governments sometimes have failed to effectively harness open data to solve, or at least start to tackle, thorny problems. These problems span jurisdictions, policy domains, and levels of government. Designing multiorganizational, multidimensional, and multijurisdictional efforts that use government data is not a simple endeavor. National policy governance for open data in Korea provides several useful insights that other national and local governments can learn from. This analysis addresses three main issues regarding Korean open data policy governance: institutions, policies, and organizational capacity.

Korea's Conflicting Institutional Landscape

An important initial consideration for understanding Korea's open data policies is the country's institutional underpinnings in this policy sphere. The Ministry of the Interior and Safety (MOIS), the Ministry of Science and Information and Communications Technology (MSIT), and Statistics Korea each oversee some aspects of Korea's open data policies. These three central agencies play different respective roles: overseeing public-sector data, private-sector data, and authorized statistical data. But because the distinctions among these three categories have increasingly blurred with the emergence of big data and the complicated nature of new data sources and data sets, Korea's institutional framework has become muddled.

This means that Korea's institutions will need to evolve to combine data from many different types of organizations. And these institutional frictions are mirrored in contradictory legal and regulatory provisions and a lack of consensus among the Korean government, corporate players, and civil society. There is, in short, an absence of effective digital leadership at the national level.

Institutional Complexity of Open Data Policy

Korea's open data challenges begin with the fact that the MOIS, the MSIT, and Statistics Korea each exercise responsibility and oversight over some elements of the country's national data management system. These three agencies institutionally differ in their main missions and roles related to open data policy. But the differences are not entirely clear-cut. When open data initiatives were initially introduced, open data meant open public data only. Since 2021, the MyData project in Korea has allowed accredited companies (known as MyData operators) to manage personal information scattered across the financial, telecommunications, medical, and public sectors.[144] This project enables the further use of data through the pseudonymization and anonymization of personal information. In this sense, the distinction between big data in the private sector and existing open public data is becoming less pronounced, and the jurisdictional boundaries among Korea's three major regulatory and policy institutions is also growing blurred.

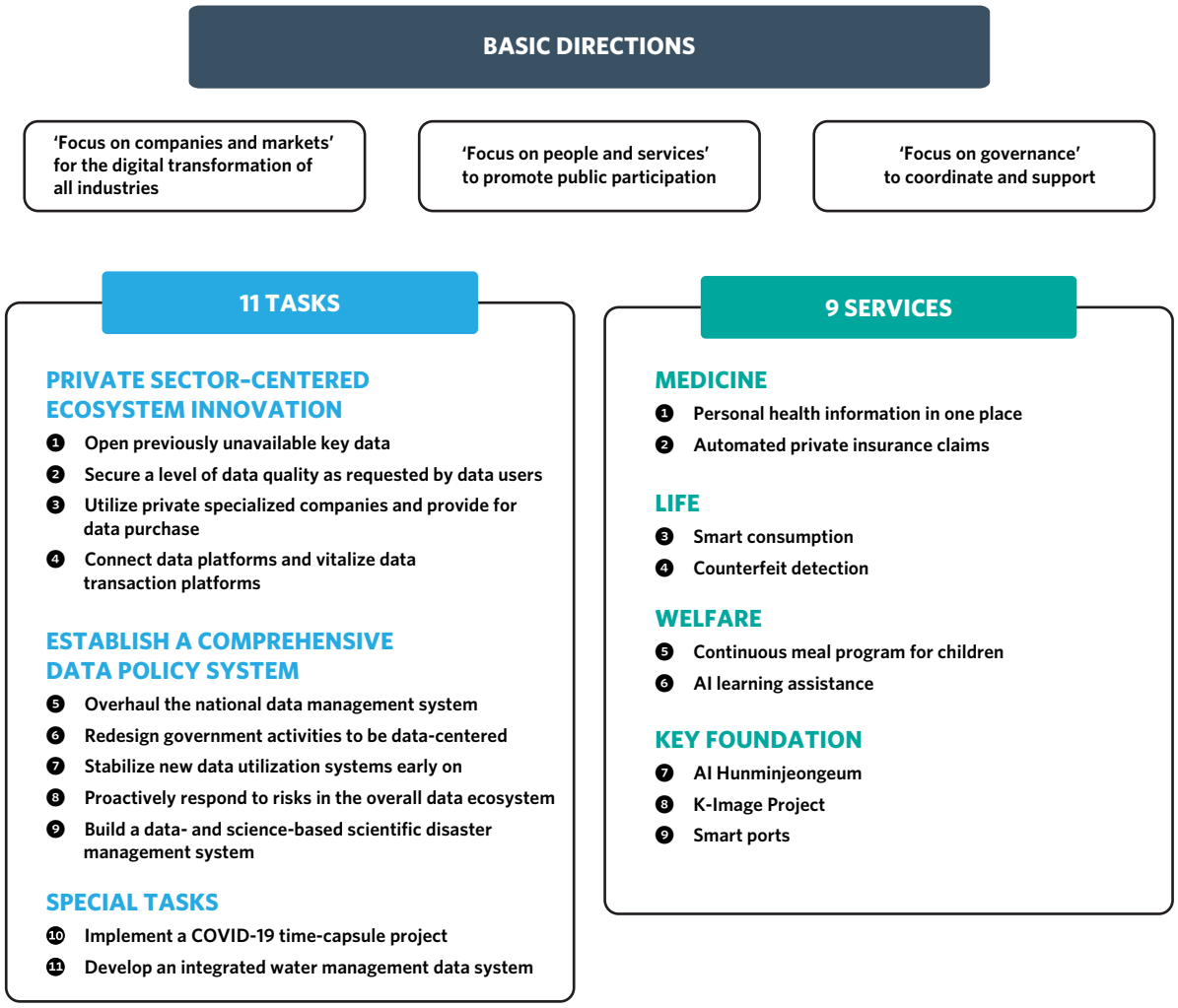
The Bureau of Digital Government (formerly known as the Bureau of e-Government) within the MOIS acts as a control tower for the digital transformation within the Korean government, and its three divisions (the Division of Open Data Policy, the Division of Open Data Circulation, and the Division of Big Data Analysis and Use) in turn administer all work related to harnessing public data.[145] The MSIT, by contrast, is the government's lead agency for data generated in the private sector, including corporate data, industry data, and research data. The MSIT's Division of Big Data Promotion helps establish data infrastructure, offers support for firms that handle data, and promotes data-related industries.[146] The third key agency, Statistics Korea, creates statistical data, runs the country's national statistics portal, and manages microdata integration services.[147]

The jurisdictional boundaries of Statistics Korea (which is tasked with the provision of official statistics) have become less distinguishable with the industry changes brought about by the rise of big data analytics. Both the MOIS and the MSIT recognize that the strict division between their data areas (data from the public sector and data from the private sector) is eroding. This institutional governance arrangement does not fit well with these rapid changes in the open data ecosystem. With the advent of big data, this ecosystem makes data even more valuable in new ways beyond authorized statistics and weakens the dividing line between public and private information.

To add another layer of institutional complexity, these are not even the only three players in Korea's open data landscape. Other government agencies also shape policies that affect open data initiatives at the national level. For example, the Personal Information Protection Commission is a powerful regulator in charge of data security and privacy protection.[148] This commission enforces Korean laws equivalent to the Privacy Act in the United States, where privacy protection is self-regulated, whereas Korea has a national control tower of privacy protection. Thus, the commission steps in when these three agencies involved with open data overstep in ways that harm citizens' privacy.

Meanwhile, the Presidential Committee on the Fourth Industrial Revolution designs and coordinates Korea's national digital policies.[149] This committee deliberates on and then coordinates important policy matters pertaining to the development and acquisition of new advances in science and technology, including artificial intelligence (AI) and data technology, as well as new industries and services necessary for Korean society to embrace the Fourth Industrial Revolution. The committee includes the Data Special Subcommittee, which consists of experts and practitioners from related ministries, industries, and academia. The Korea Data 119 Project, which strives to harvest and harness ideas from the private sector, seeks to promote the opening, distribution, and utilization of data.[150] Figure 3 shows eleven tasks and nine services conducted by a specific ministry or through collaboration between ministries. The three aforementioned key institutions play especially important roles in these eleven tasks.

Figure 3. Korea's Approach to Data-Driven Innovation



Source: The Presidential Committee on the Fourth Industrial Revolution, "Data 119," The Presidential Committee on the Fourth Industrial Revolution, https://web.archive.org/web/20220613225537/https://www.4th-ir.go.kr/en/data119.

Meanwhile, the Open Data Strategy Council, which is co-chaired by the prime minister and a data expert from the private sector, designs the basic plans for opening public data and improves these plans to assure better usage of public data.[151] This council is a deliberative body that examines, coordinates, monitors, and evaluates government decisions and the implementation of major open data policies and plans. The MOIS formulates and refines the open data master plan, evaluates implementation, creates the relevant infrastructure, and releases data. Participating organizations under the council play other specific roles. To cite a few examples, the Open Data Center for Policy and Technical Support provides technical assistance

and acts as a hub and clearinghouse for open data,[152] the chief open data officer in charge of providing public data leads open data efforts at all public organizations, and the Open Data Mediation Committee handles disputes over public organizations' refusal to share data or decisions to stop data sharing.[153]

Legal Conflicts

This diverse array of institutions must operate within a legal and regulatory framework that, unfortunately, has some inherent conflicts and contradictions. Specifically, Korea's data-related legal frameworks include the Framework Act on Intelligent Informatization,[154] the Personal Information Protection Act,[155] and the Act on Promotion of the Provision and Use of Public Data.[156] Reflecting a massive paradigm shift powered by AI-driven societal changes, the Framework Act on Intelligent Informatization is a revised version of the Act on Informatization, which has been a legal foundation of national informatization in Korea since 1995.

Korea's bureaucratic diversity has been replicated in these laws and regulations. For instance, the MSIT is responsible for implementing the Framework Act on Intelligent Informatization, but the MOIS is responsible for implementing the Act on Promotion of the Provision and Use of Public Data. This regulatory diversity, in turn, has created confusion and potential conflicts. Yet no one law specifies which government body or bodies have the jurisdiction to manage the data that the private sector generates.

The same is true when local governments become involved. For instance, Korea's current law on informatization requires all provincial and local governments to submit their basic plans for informatization (including open data) to the head of the MOIS because this official formally controls the local autonomy system in Korea, but the minister of the interior and safety must then provide these local plans to the minister of science and information and communications technology (ICT).

As a result, these two ministers need to coordinate and collaborate. This can be a tall order, however, because public data (under the MOIS) cannot be easily integrated with private data (under the MSIT) since the two different ministries' jurisdictions may functionally overlap but remain institutionally divided. Invariably, then, these related laws can and do yield inevitable conflict among several different ministries.

Legal Rhetoric on Data-Driven Administration

The Act on the Promotion of Data-based Administration legally and institutionally gave rise to data-related processes, procedures, and resources.[157] This formal support of data-driven administration highlights all data-related government processes, including excavation, collection, processing, registration, and reuse of data. The act stipulates that all Korean government agencies must designate a chief data officer and have an organizational unit dedicated to data-driven administration. But the right people—those with relevant expertise—are infrequently recruited for these jobs. A starting point of all data-driven administration is making government data available to the public. Unfortunately, most government organizations, including in Korea, find it easier to define a vision and write a plan than to substantively increase openness.

Open public data is not the same as freedom of information requirements, although both necessarily require that government officials be transparent. Open data must have tangible benefits (and not necessarily financial ones) from further data use in industry, academia, mass media, and the public sector, whereas freedom of information programs must satisfy citizens' constitutional (unavoidably abstract and symbolic) right to know certain information. Korea's approach to data-driven administration tends to tout the idea that the country is opening as much data as possible, but that is simply not sufficient. Such rhetoric fails in practice because it does not provide well-defined criteria for success to guide the wide variety of actors who use and leverage data.

Without clear goals, Korea's government will struggle, as many governments do, to work with nongovernmental organizations. Government employees who deal with public data need to be able to understand and explore the full range and richness of the data that different and diverse ministries capture. In many countries, not just in Korea, it is wrongly thought that the success of open data initiatives can be measured by simply counting the number of available data sets. Or else government-led open data initiatives showcase process flow charts and increased throughput instead of generating substantial societal benefits. This has been a clear challenge in Korea, too, as many corporate data users complain about the low value of open public data (due to its incompleteness, poor quality, lack of timeliness, or limited significance). Even government employees do not have a substantial understanding of what data-driven administration means and why it is important for the public sector, much less the country's corporate and academic sectors.

Institutions Lag Behind Technologies

A related problem is that Korean laws and institutions do not always reflect the scope and intensity of technological change. Take, for instance, the Act on the Promotion of Data-based Administration, which on the surface would seem to demonstrate institutional readiness for wide-ranging, technology-driven changes.[158] Both the executive branch and the legislative branch of the Korean government have passed several ambitious, innovative laws and regulations to this effect. Another is the Electronic Government Act,[159] which was the first of its kind anywhere in the world. The Act on the Promotion of Smart City Development and Industry,[160] the Framework Act on Intelligent Informatization, the Act on Promotion of the Provision and Use of Public Data, and the Act on the Promotion of Data-based Administration likewise aim to enable the societal changes and government innovation made possible by cutting-edge technologies. Korean legislators recognize the need for frequent revisions to these laws as new opportunities and challenges arise. For example, emerging technologies and new business models have shortened the cycle for necessary legal revisions. The executive branch and the National Assembly have revised laws quickly in response to emerging technologies. Interestingly, they aim to write proactive legislation, which is designed to remain effective not just today but also in the near future and over the long term.

But future-proofing legislation amid the blistering pace of technological change is never easy. Legal language, institutional culture, and organizational capacity do not always align. Well-designed legislation and regulations need to be paired with adequate budgets and staffing to provide the flexibility needed to adapt policy to new opportunities and challenges.

The trajectory of technological change and the policies that shape this arc are not preordained. Academics (and not just scholars in fields related to ICT) and government practitioners know that technological progress is not deterministic. They recognize that their actions can create new technological pathways, though they likely cannot truly or fully grasp the complexities of theories that try to combine sociological determinism and technological determinism or how those theories can guide their decisionmaking. Given how difficult it is to accurately predict the pace and scope of the development of technologies and relevant applications, much less their ultimate societal impact, public attitudes toward technology, whether technology-fueled optimism or a technology-driven backlash, can have more influence than rigorous analysis.

Over the last two decades, Korean legislation has had to be repeatedly and frequently updated to reflect changing social attitudes toward digital technologies. Recent laws were inspired by technology-based, hyper-powered optimism about open data. But because technologies have evolved faster than governments, businesses, and societies, institutional design by necessity has been and will continue to be modified frequently. While it is inevitable that some institutions will lag behind technologies, problems are bound to arise when open data authorities fail to be flexible and future-minded enough to deal effectively with the consequences of this lag.

A Bias Toward a Positive Regulatory System

Traditionally, Korea has featured a strong push for a positive regulatory system. Simply put, positive regulation lists what actors can do, while a negative regulatory system describes what they cannot do (a regulatory sandbox). The former enables interference, while the latter aims principally to prevent interference. For the former, the government intervenes to force the market to do only the specific tasks outlined in the regulation. In contrast, negative regulation imposes restrictions on the basis of law and bans or punishes certain actions.

In Korea, when government agencies have confronted emerging technologies, their reaction has nearly always been to establish positive regulations and thus to confine and bound the role and scope of the market. After all, all regulations ultimately have two purposes: encouragement (and promotion) or prevention (and prohibition). Data-related laws in Korea primarily seek to promote data-related industries and economic sectors. However, Korean corporations tend to recognize that the government institutions implementing and enforcing these regulations can matter as much as the words themselves. By means of an illustration, if a single data set on an open data portal is to be more meaningful, the data set should be aligned with other data, even data from the private sector. A firm may wish to use customer data from other firms, but Korea's legacy of positive regulation does not attempt to monitor and regulate the results of using such integrated data (ex post regulation) but rather prospectively specifies who uses what data, from which different sources, and for what purpose (ex ante regulation). The result often is undesirable conditions for potential data users.

Discretion in Institutional Interpretation

Korea's Act on Promotion of the Provision and Use of Public Data controls the data that all public agencies have, but this does not mean the law is applied to each agency in the same manner.[161] Indeed, the nature of data and related processes (including data collection, storage, processing, analytics, and use) may differ between agencies. This dynamic results in a significant difference in institutional discretion in interpreting the act. For instance, while some Korean ministries are mostly focused on data stewardship, others strive first and foremost to facilitate more extensive use of data. Even within the same ministry, different bureaus can have different approaches to opening up data sets. Expectations from open data and the further use of open data can differ among government organizations. Differences in institutional interpretations also arise from asymmetries, which are common at the level of data access and in terms of expertise between different parties (including industry peers, industry and government, peer government bodies, and citizens and companies).

For example, defining what qualifies as personal data is not clear in some cases. Because of that, most decisions have ended up with an overly broad definition of personal data. There are guidelines that define a general strategy for the use of open data. But because these guidelines do not clearly specify what is possible or conversely what is not allowed, there are discretionary decisions about what data should be open and how this data should be shared. This leads to public confusion: external users of open data often ask why this data is open in one ministry but not open in another ministry. The Korean government's bureaucracy has often showed that when tensions between data protection and data sharing arise, a conservative stance commonly prevails.

Policy Governance Issues

These various institutional, legal, regulatory, and other features are key parts of Korea's model for governing open data. But a country's bureaucracies, institutions, and laws are not the only relevant considerations for assessing its stance on open data. Its approach to governance matters too, and this is equally true in the case of Korea.

Cross-Government Policy Coordination

The leading agency tasked with managing public data (the MOIS) is different from that for managing open data (the Open Data Strategy Council), and open data actually seems to mean activities for opening up public data. An important definitional component of the open data concept is use by anyone for any purpose, but too often Korean open data initiatives focus on being government-led efforts for the public interest. To realize the full potential of open government data and to see visible, measurable, and provable improvements, there needs to be a renewed focus on letting any party use data for any purpose within reason.

To this end, Korean government agencies need policy coordination across their functional and jurisdictional boundaries. Digital leadership at the national level entails collaboration among different ministries and even with nongovernmental parties. In this sense, Korea needs a clearly identified and strongly empowered coordinating body for open data policy.

A Missing Governing Body

Korea quite simply lacks a unitary national institution for data management and control, which, in turn, makes it difficult to move and share data across sectors, domains, jurisdictions, and organizational boundaries. To a casual observer, the lack of such a body makes the country's open data management system look fragmented, but the real problem is not a failure of institutional design but a failure of national-level data policy governance: this is because in the Korean government structure, one agency cannot impose policies on multiple ministries.

To remedy this problem, Korea has considered establishing a new ministry-level data agency, but the performance of any such agency would invariably depend on the attitude (and cooperation) of other existing ministries, which continue to resist this idea. An ongoing issue is who should manage the relationships among ministries related to open data.

The Legacy of Korea's Public-Private Dichotomy

Historically, Korea's public and private sectors have been clearly distinguishable. As a result of that legacy, the separation between public data and private data has been unnecessarily strict. A monumental exception was the early response to the coronavirus pandemic. Contact tracing for confirmed cases required the authorities to tap private data (such as telecommunications data and credit card data), which are purely personal data and owned by corporations.[162] But the successful use of this private data directly and entirely supported the public interest in slowing the spread of COVID-19. The legacy of this sudden shift in 2020 is that Korean government agencies, private corporations, and civil society organizations have started to rethink the scope of open data and how it can be used.

Still, the dichotomy between public and private data is apparent in the world of open data. As a result, both the MOIS and the MSIT take an integrated, society-wide view of public and private data, but their respective jurisdictions reflect the legacy of Korean institutional design and governance practices and history. What is more, this separation into public and private spheres under two different agencies also impedes organizational and sectoral collaboration and erects barriers to generating new value from data integration.

Big Data Crowds Out Statistics

Statistical data also factors significantly into Korea's emerging open data regime because it plays a crucial role in spurring economic growth, industrial development, and policy formation. With the emergence of big data, the role of government-tallied statistical data is shrinking.

In Korea, almost all of the government's statistical data—whether at the national, provincial, or city level—are open data. The authorized government data are validated by the national statistics office, but this process inevitably takes time. As a result, many academics and researchers use open data from Google, not official data from the Korean government. This raises the question of whether the big data compiled from Google can be considered accurate and valid for such users.

The scope of open data obviously expands with new technologies. Authorized statistical data are still important, but new sources of easily accessible open data are complementing and even supplanting official statistical data. Government agencies, businesses, and researchers inevitably have to decide how much to trust and rely on different sources of data and how to differentiate between reliable and unreliable sources. Given this situation, integrative and collaborative governance should consider both statistical data and nonstatistical data and how to combine and leverage both. Statistics Korea has a unique jurisdiction, but the Korean government should consider restructuring it to make it a governing body for managing open data.

Korea's Open Data Conundrum

But Korea's biggest conundrum and challenge with open data is for the government, in shaping data policy, to both protect sensitive data (such as personal information or data related to national security or law enforcement) and make data available in useful formats for a wide range of applications. Different nations provide different levels of data protection (for different reasons), yet they all face this conundrum. Korea is no exception.

The Open Government Partnership encourages member countries to learn from one another's open data strategies and share their successes and failures.[163] One performance metric involves counting the number of data sets that are open to the public via webpages, but that is not the only one. That metric merely measures input, not output. What is needed for performance management of open data efforts, therefore, is rigorous analysis of what is actually accomplished and how open data are used, for whom, and for what. If useful data is not made available in useful ways, it will provide little value.

The Korean business sector has taken a particular interest in this issue, not least by questioning the value of many of Seoul's official open data initiatives. Korean data practitioners in the business sector often complain that there are simply few data sets of value on the country's open data portal, where many data sets make it difficult to create new opportunities for industries, businesses, and academics. The data sets in the government's open data portal are composed of many smaller ones that could have been stitched together, have many missing data points, and cannot easily be synced to match the formatting of others. It is time for government bureaucrats to change their approach and their attitudes. They need to focus on high-value, open public data and help market it to prospective users. This could help change the common perception in Korea that open public data tend to be low-value data.[164]

Potential business users and researchers, in particular, can help push government agencies to make more open data available. If they wish to have access to truly meaningful data, they should make additional efforts to file freedom of information requests. To some, this may seem like an unusual approach, but open data initiatives and freedom of information legislation have a similar goal: more transparency and more useful insights from government agencies.

Of course, freedom of information requires one to make requests by filling out a form. Requesting information in this way is not like using a vending machine: there are various reasons, after all, that a government agency can reject such requests. Or some pieces of requested information can be redacted and masked with exemptions. It may be very hard to gain a perfect or complete data set in certain cases. If the data is about internal government operations, agencies often do their best not to give the requested information. But filing freedom of information requests not only makes more data available but can also create political pressure and ultimately motivate government agencies to make more data available (even without requiring time-consuming requests).

Korea needs a strong governing body that can juggle the tensions between the need to protect some data with the need for more access to data. Currently, Korean government bodies lack incentives to facilitate data use, and they worry about additional responsibilities, accountability, and criticism that might result from releasing data. The country's national governing body must be able to let all government agencies recognize the social benefits and multidimensional effects that open data initiatives can produce.

Conflicting Priorities Across Organizations

The conflicting goals of data protection and data use are not only reflected throughout the Korean government's data policies: this disconnect also complicates decisionmaking within agencies. Within a single ministry, different offices can have different priorities and different constituencies. For instance, the Ministry of Health and Welfare, which manages huge amounts of valuable, healthcare-related data, must juggle the need to support the further use of personal medical data and promote the healthcare data sector (data use value) with the need to protect patients' personal healthcare data (data stewardship value). The ministry is not inherently in conflict with other agencies on the matter of data use, but it has internal conflicts within its own four walls. One such conflict concerns who owns data related to diseases: Is it the patients themselves? Or does it belong to hospitals and healthcare professionals? Or is it part of the national healthcare system? Or could it even be all of the above? Who owns or controls healthcare data depends on who creates the data, what contractual obligations they have, and what legal restrictions limit its use—and that all affects what kind of value is generated from such information.

Poor Communication on Open Data

As of now, the Presidential Committee on the Fourth Industrial Revolution is in charge of national open data policy in Korea, and it has to mediate among different stakeholders with a variety of viewpoints on open data.[165] The committee endeavors to listen to voices in data-related industries, but these voices

reflect the interests of different sectors and can have very different priorities. Similarly, it can be hard for individual government agencies to ensure effective communication and collaboration between firms that need data and the offices that can provide it. And governments need to listen to and address the needs and concerns of individual citizens, too.

For Korea, this means that designing good data policy will require deeper, more effective communication between policy designers and all policy beneficiaries. Social media platforms and other interactive communication channels tend to be more effective at expressing their needs to the government than enterprises in traditional industries often are, but those communication channels can also provide collaborative tools to enable other stakeholders to express their views.

Korea's Inactive Open Data Ecosystem

Data users, especially firms, often have a passive attitude toward open data. This attitude, in turn, reflects a lack of investment, interest, and even imagination. The commercial data industry is not as highly developed in Korea as it is in the United States.[166] So the government's role will be critical for creating a more favorable environment for the data industry and improving policies related to open data.

One challenge is that Korean firms and nonprofits need to be ready to find new data sources and extract new value from such data. Unfortunately, most Korean firms have discovered very little of the potential value from open government data, which is free and available from government agencies via the open data portal. Open data is categorized into specific policy domains (by ministries, public agencies, and public corporations) and government jurisdictions (by province and locality). But many users would prefer to see data across industries, across ministries, and across jurisdictions, and the current focus of Korea's approach to open data is often little more than releasing the data that each public agency is willing to publish. When a Korean government agency determines which data should be open, it too often does not consider how to make sure the data can be used to create new value through the integration of data from different ministries and other forms of nongovernmental data. The main actors in Korea's open data ecosystem are public agencies, who measure their progress by the number of data sets uploaded and downloaded. Open data has simply not been thought of as an ecosystem of relationships among multiple actors, one that touches and connects all sectors of society.

Korea's Organizational Capacity Challenges

Korea faces some pronounced issues of organizational capacity that it will need to remedy to maximize the efforts of its open data ambitions.

Bureaucratic Dysfunction

Korea's governance structure for open data is a barrier to making more public data available. Functional and organizational inefficiencies in the country's national data management keeps agencies from facilitating open data projects. The rule of law is the foundation of democracy and good governance, and this is no

less true in Korea. But public officials in the country often abuse the principle either by highlighting institutional measures for enforcing a law rather than the underlying spirit and intention behind the law or by using outdated or vague regulations as an excuse for inaction.

Oftentimes, the rule of law is not the problem, per se. Instead, public officials misconstrue the implementation of a law, especially when the law's scope is restricted to a specific area and is in conflict with broader government mandates to share data. Korean government agencies often forget the ultimate purpose of policy (what the law originally purports to do). All organizations tend to strive to keep and even broaden their turf. Thus, in Korea's case, for example, different government bodies are responsible for the implementation of different data-related acts: the MSIT is in charge of implementing the Framework Act on Intelligent Informatization, the MOIS takes charge of implementing the Act on Promotion of the Provision and Use of Public Data, and implementing the Statistics Act is basically a core function of Statistics Korea.[167]

Despite this parceling out of duties related to data governance, areas of overlap and duplication are inevitable, and these areas are increasing. Although having one agency, one law, and thereby one mission is the ideal, that is not the case in Korea today. When there is no agreement on who is responsible for what, bureaucratic inertia and classic infighting results. In that sense, open data governance suffers from the same bureaucratic problems that plague other government functions: a government office may try to push some data-related work off its plate onto another office, or an office may try to seize control of other data-related tasks away from another office. As a result, inefficiencies and missed opportunities can arise from both governing hot spots (areas rife with overlapping administrative efforts by competing ministries) and dead zones (areas without governing activity in which relevant offices try to avoid getting involved).

A Siloed Work Culture

As in most governments, the traditional bureaucracy in Korea tends to be stovepiped, making it difficult to horizontally share and integrate data and information. The central government's ministries have established, developed, and advanced their own systems, including information systems, databases, and software systems. A better, more consolidated cross-agency system for data management and policy development is badly needed.

The Korean bureaucracy holds ministerial data according to the legal rationale for which a respective ministry exists. The rule-of-law principle in Korean public administration seems quite distorted or abused because sometimes bureaucrats cannot think beyond the law itself. A prevalent issue among Korean public-sector employees is "inactive administration."[168] They do not consider the fundamental, original purpose of a law, but rather use their discretionary interpretation of the law according to their institutional preferences and what is convenient. The country's bureaucracy was well-designed to address issues and solve particular problems defined in the law. However, ordinary organizational behaviors look very different from their design. Despite the necessity of cross-boundary data integration, it remains challenging work that is often considered out of ministry personnel's jurisdiction.

Data integration requires all related organizations to be functionally connected, but the Korean system is beset by barriers. Meanwhile, even as government agencies struggle to overcome structural impediments to collaboration, data users are struggling to access meaningful information from publicly available open data. This, too, is difficult because siloed Korean ministries, in turn, have created siloed data sets.

A critical issue, therefore, is not whether Korea has a national portal site for opening public data—indeed, the country already has one—but rather how to make organizational silos actually open so that this data can be meaningfully integrated.

Improving Organizational Capacity

Beyond fixing Korea's bureaucracy, however, the country also needs to improve some of the organizational obstacles that are impeding an open data regime. Job recruiters and headhunters complain about the paucity of data experts in the country.[169] And while Korea's national government, much like its counterparts everywhere, understands the importance of data expertise and assertively recruits such expertise for the public sector, private sector organizations, including even high-profit firms in the tech sector, struggle to find relevant professionals and practitioners in data-based fields. Both sectors, public and private, are still struggling to do so. A shortage of people with the skill sets to deal with open data is a critical issue. Indeed, Korean government offices at every level—central ministries, provinces, and localities alike—lag behind the global leaders in data gathering, data storage, data analytics, and data use.[170] Furthermore, local governments face an even more serious gap in organizational capacity than the national government, while smart city initiatives increasingly highlight open data projects.

Korea will need to get more serious about this challenge if it wants to be a global leader in open data. Despite the Act on the Promotion of Data-based Administration's requirement that all Korean public sector organizations designate a chief data officer, in most public organizations, that position is actually concurrently assigned to someone who may hold another post and may not have the typical technical expertise of a chief data officer. Dedicated data professionals are very rare in the Korean government,[171] and well-paid data practitioners in the private sector are often reluctant to work for the public sector.

As a result, Korean public organizations have outsourced jobs related to informatization, technological innovation, and more recently digital transformations (such as the adoption of AI, the use of big data analytics, and the transition to cloud computing) to the private sector and academia. This public-sector dependence on nongovernment parties is not automatically disadvantageous (since outsourcing does bring advantages, including flexibility and nimbleness). But the ever-widening gap between the unchanging bureaucratic core of the Korean government and innovative corporate expertise has put the country's public sector at a considerable disadvantage.

To bridge this gap, the Korean government has promoted an approach to governance premised on collaboration among public and private actors. It has, for example, outsourced many service-delivery tasks. But it has also sought to ensure that decisionmaking about the digital transformation is informed by corporate experts, industry leaders, and academics.

Korea has some notable public-private partnerships of this type. That is why the country ranks high in the United Nations' e-Government Readiness Index and the Organisation for Economic Co-operation and Development's Digital Government Index.[172] However, this intensifying gap between the data expertise available to Korea's public and private sectors is making the government fall behind in terms of how effectively organizations integrate data across organizational boundaries and how they increase the usability of open data for the public.

The outmoded recruitment and promotion practices of the Korean bureaucracy may be an enduring impediment to open data unless countervailing steps are taken. The bureaucracy tends to hire most government employees using a national open examination, which works better for recruiting generalists than specialists. These generalists do specialize as they move along their career paths, but very few end up with the industry-specific domain expertise that private-sector employees gradually acquire. Instead, most Korean officials become adept at navigating the organizational intricacies of the government. For instance, good public managers in one bureau could conceivably move to a director position in another bureau.

Of course, Korea's public-sector personnel management system is more sophisticated, varied, and flexible than can be depicted in a few paragraphs. But this system poses a challenge to creating a truly world-class open data regime for several reasons. First, data manager positions are often not filled with data experts who possess expertise equivalent to data managers in the private sector. Second, the Korean government's generalist personnel culture encourages circulation between jobs to provide for more diverse experiences and to avoid regulatory capture and corruption, so employees usually change roles every one or two years. As a result, government employees in data-related posts also cannot hone their own expertise throughout their career. Third, one of the most important motivations for Korean government employees is the opportunity for promotions to higher managerial positions, which means they do not want to remain merely data workers.[173]

One option would be for a single unit or team within a given agency to try to take charge of all data-related work. But even that approach has advantages and drawbacks. One problem is that most employees do not know all the different offices and people who could be involved in data-related work. Many data sets in Korea's open data portal do not capture various aspects of government operations and public service delivery. And there are many cross-sectional open data sets that were not made with the long term in mind. In most cases, periods of missing data result from poor organizational capacity, especially a lack of good data sense. For example, sometimes government employees seem not to understand why certain data should be provided to the public and who would potentially use it.

Learning From Korea's Struggles

This analysis has discussed more challenges than opportunities facing Korea in terms of open data governance. But ironically, the discussion should not leave a negative impression of the future of open data; rather, other countries can learn from Korea's recent self-reflections about its trials and experiments.

The Korean government is a key leader and coordinator of open data governance at the national level. The inevitable lag of institutional readiness behind rapid technological change, organizational obstacles stemming from bureaucratic inertia, and the gap between the legal code itself and actual implementation are all evident in Korea's efforts to improve its open data governance. All countries may have similar concerns and challenges to some extent. An important lesson from the Korean experience is that open government is vital to open data. But executing the vision is not easy precisely because government actors that champion open data may not actually open their own data for the cause.

Open data should be considered a process, not an end in itself. As Korea's experience shows, given the pivotal role of national governments in open data, the rest of the world can learn from the pains Korea has weathered and leverage that experience to craft a better governance system for open data policy.

CHAPTER 3

What's Shaping India's Policy on Cross-Border Data Flows?

SMRITI PARSHEERA

Introduction

A 2019 report by India's Ministry of Electronics and Information Technology predicted that India could have a $1 trillion digital economy by 2025.[174] It also acknowledged that this growth potential could only be realized if the country creates an enabling environment of policies, platforms, and partnerships suited to the "borderless" character of the digital world, in which "capital, innovation, data, and design capabilities flow . . . to countries that offer the fewest pain points."[175] But, despite these acknowledgments, the report did not remark further on the relevance of cross-border data flows for meeting its digital ambitions.

Yet the question of how to manage cross-border data flows is central to India's digital future. After all, it is a country that has reaped significant benefits from being digitally connected and following an open market policy in this space, with the free flow of data being an integral part of that equation. But at the same time, it is also a country that is increasingly grappling with the challenges posed by unchecked data extraction, data monopolization, and barriers to lawful data access.

This dilemma has prompted a new wave of policy thinking, as reflected in debates on data governance and digital regulation, that signals India's ambition to transition from a user to a controller of digital markets. India's strategy of technological self-reliance combined with its frequent assertions of digital sovereignty are also reflected in its approach to cross-border data flows.[176]

Over the last two decades, India has benefited immensely from open practices enabling free cross-border data flows and the import and export of digital services. According to one study, digital trade generated $35 billion in economic benefits for India in 2019, and that figure was projected to rise to $512 billion by 2030, an amount equivalent to 10 percent of the country's projected gross domestic product (GDP) at that point.[177] At the same time, it is undeniable that the social and economic benefits of digital development are not evenly distributed within societies, between private actors, and among countries. To give an example, the revenues of six major U.S.-based technology companies in 2021 exceeded $1.4 trillion,[178] which is more than forty times the size of India's estimated benefits from digital trade in 2019. The data advantage that these large global players enjoy is a crucial component of their economic success.[179] This realization is coupled with the limitations of regulatory and law enforcement control over international actors, concerns about privacy and security, and visions of supporting greater economic benefits for local companies. The confluence of all these factors has propelled state actors, in India and globally, toward more restrictive regimes on data flows.

A report by the Information Technology and Innovation Foundation recorded a recent surge in regulatory requirements focused on data localization. These include directives that data be stored and/or processed within a country's territory, either on an exclusive basis or through the local mirroring of data that is stored elsewhere. Whereas thirty-five countries had sixty-seven localization requirements in 2017, the authors found that there were sixty-two countries with 144 data localization restrictions in 2021.[180] The report found that India has the second-highest number of such restrictions (behind China), including in areas like financial services, the provision of cloud services to government agencies, telecom subscriber data, company accounts, and public data.[181] In addition to the measures already in force, a number of localization proposals are in the pipeline, most notably under India's proposed data protection law, though this draft has been withdrawn for now.

The subject of cross-border data flows has also moved front and center in several international forums. This includes attempts at building a shared plurilateral position on data flows under the Group of 20's (G20) Osaka Track and as part of the Joint Statement on Electronic Commerce initiated by a group of countries at the World Trade Organization (WTO).[182] In addition to data flows for commercial purposes, new arrangements to enable access to data for law enforcement are taking shape through mechanisms like the Second Additional Protocol to the Budapest Convention on Cybercrime[183] and the United States' Clarifying Lawful Overseas Use of Data Act.[184] Further, a 2019 United Nations (UN) resolution has paved the way to developing a treaty for "countering the use of information and communications technologies [ICT] for criminal purposes," which will also cover issues of data access.[185]

India's presence in forums like the G20 and the Global Partnership on Artificial Intelligence gives it the opportunity to be at the forefront of key international conversations on digital governance. Its position on data flows, however, stands apart from those of the other G20 members, most of whom have chosen to pursue international discussions on data flows under the Osaka Track.

India's stated reasons for this difference revolve around its desire to maintain the space to formulate domestic policies on issues of digital governance and an insistence on more inclusive and multilateral decisionmaking. India's position on data flows is also influenced by its roots in forums like the Group of 77 (G77) and the BRICS coalition alongside Brazil, Russia, China, and South Africa that allow New Delhi to represent developing and emerging world powers' responses to the dominance of developed nations, including on matters of technology. But interestingly, and unlike India, others including China and Russia that also belong to the G77 or the BRICS have nevertheless opted to be a part of the Osaka Track. This suggests that, although India routinely relies on its groupings with other developing and emerging countries to assert its positions on issues of digital governance, such platforms may be more of a place to anchor its positions rather than the strategic impetus that brought the country there.

This analysis traces the main instruments and arguments that are driving India's position on cross-border data flows with respect to domestic policies and international forums. It highlights how India's unique position in this debate is being shaped by a mix of evolving domestic priorities and the multiple identities that the country straddles on the international stage.

The first section of this analysis outlines the actions and instruments shaping India's current and proposed restrictions on cross-border data flows. The second section presents an overview of the drivers of data flow restrictions in India, as laid out in expert committee reports, regulatory directives, and other policy documents. The third section widens the lens of analysis from a local perspective to a global one by outlining the strategic and geopolitical dimensions of India's participation in international conversations on data flows. The next section then looks beyond the issue of commercial data transfers to focus on the actions India has taken to facilitate law enforcement access to data through mechanisms like mutual legal assistance treaties (MLATs). The final section concludes with some suggested paths for reform.

India's Current and Proposed Restrictions on Data Flows

Numerous policy documents have articulated the role of data in India's socioeconomic development. This includes various forms of data, including personal and nonpersonal data, and data for various use cases, ranging from government functions to commercial purposes. In general, these discussions focus mainly on the benefits and risks of data processing and the need for regulatory or technical solutions to strengthen India's data infrastructure.

But references to cross-border data flows tend to be rarer and are usually limited to proposed limitations on such flows, including in the form of localization norms. In this process, the real but invisible role of cross-border data flows in the success of India's digital economy tends to be overshadowed by the equally real challenges posed by unhindered data flows, particularly for regulatory and law enforcement purposes.

For instance, the Indian Economic Survey of 2018–2019 dedicated a chapter to discussing the many benefits of data for policymaking, welfare delivery, and product innovation.[186] It noted that these benefits are spurred largely by the decreasing marginal costs of gathering, storing, processing, and disseminating data. However, the chapter made no specific reference to the current market realities of cross-border data flows and the role they play in lowering the marginal costs of data storage and processing. Recent policy conversations—informed by the findings of the Gopalakrishnan Committee, which was set up by the Indian government in 2019 to develop the regulatory structure for nonpersonal data—follow a similar trend.[187]

The committee's report speaks at length about the public benefits that can come from unlocking access to nonpersonal data (meaning information that is not personally identifiable, including anonymized personal data) and suggests a new regulatory structure to enable data access by government agencies and organizations registered in India. While discussing the process of value creation from data, the committee did not account for the role that cross-border flows have historically played and continue to play. Their treatment of the international character of data focused only on the data pools held by large multinational corporations and the resulting market dominance they hold.

The issue of cross-border flows has been more central in ongoing discussions on the regulation of personal data. A draft piece of legislation called the Personal Data Protection Bill, 2019, was introduced in the Indian parliament in December of that year, and a further modified version of the bill—the Data Protection Bill, 2021 (DP Bill)—containing the recommendations of a joint parliamentary committee was submitted in 2021, though the bill was subsequently withdrawn (see below). The bill contained several restrictions on cross-border flows, proposals that originated from the recommendations made by the Committee of Experts Under the Chairmanship of Justice B.N. Srikrishna (or the Srikrishna Committee), which prepared the first draft of the bill in 2018.[188] In August 2022, India's minister of electronics and information technology announced the decision to withdraw the pending bill.[189] It is supposed to be replaced by a new draft, details of which are not yet publicly available, in the coming months.[190]

The Srikrishna Committee emphatically recognized that the "flow of data across borders is essential for a free and fair digital economy."[191] But the committee also noted that data flows cannot be seen as an "unadulterated good" as unchecked data transfers can generate substantial harm to individual privacy. The committee accordingly went on to suggest expansive restrictions on data flows, which included a requirement to maintain a live mirrored copy of all personal data in Indian territory. While the scope of the restrictions suggested by the Srikrishna Committee was curtailed in subsequent drafts of the bill, the implications of localization simultaneously evolved in light of other changes in the legislation. This includes the possibility of granting broad exemptions to select government agencies, such as law enforcement bodies, from "all or any" of the provisions of the draft law and the requirements relating to mandatory sharing of nonpersonal data.[192]

The Srikrishna Committee's report cast the spotlight on data localization. The body of work that has emerged since then includes studies examining the motivations and policy processes behind localization,[193] those questioning the framing of the debate in terms of economic value,[194] and attempts at quantifying

the effects of localization.[195] Alongside this work, researchers have also examined the barriers and challenges of cross-border data access specifically in the context of law enforcement and the U.S.-India trade relationship.[196] Building on this background, it is important to consider India's internal moves and international positions on cross-border data flows both for law enforcement and commercial purposes.

Table 1 at the end of the chapter summarizes India's restrictions on cross-border data flows as seen in various policy instruments and recommendations. It displays the type of data that is covered, the nature of the restriction, and the agency responsible for suggesting or implementing it.

Table 1 shows that India's current restrictions on data flows can be grouped into four sectors or categories of data: data pertaining to financial services, data of telecommunications and broadcasting subscribers, corporate and compliance data, and government data. In addition, there are some cross-sectoral requirements, such as those pertaining to keeping logs of all ICT systems in India for 180 days and other policy proposals containing local storage and/or processing requirements for specific types of data.[197] The proposals related to the regulation of personal and nonpersonal data stand out among them, in terms of the omnibus cross-sectoral nature of the proposed laws and the range of entities and individuals that would be affected.

However, the history of the localization debate in India indicates that not all proposals may translate into actual restrictions, at least not in the form originally proposed. As noted earlier, this has been the case with the localization recommendations in the DP Bill, which have gone through several iterations since the proposal was first raised by the Srikrishna Committee. Table 1 references two other examples from the healthcare and e-commerce sectors—the proposal for a Digital Information Security in Healthcare Act and the Draft National e-Commerce Policy—where it appears that the relevant agencies have decided not to act on these proposals for now.[198] Yet it may be that the pursuit of localization has not been abandoned in these cases but only delayed with the expectation that the impending governance proposals on personal and nonpersonal data will take care of these interests. There are also other examples where the issue of local data storage came up for discussion but did not materialize as a concrete proposal, such as in the case of the National Telecom M2M Roadmap.[199]

The Drivers of India's Position on Cross-Border Data Flows

In previous work co-authored with Rishab Bailey, this author noted that the arguments for and against cross-border data flows (or data localization more specifically) can be divided into three main categories: "civil liberties," "government functions," and an "economic perspective."[200] It is important, therefore, to describe each of these perspectives, placing them in the context of the arguments invoked in the policy instruments discussed in table 1.

This discussion needs to be prefaced with two overarching observations. First, these three categories are not mutually exclusive. On the contrary, they tend to be fluid and interconnected in the sense that the same action may have consequences that fall under more than one category. For instance, while the logic of data localization for easier law enforcement access is categorized under the government functions

category, this consideration is also intrinsically linked to civil liberties. Accordingly, policy documents often invoke more than one perspective for the same action and may also call for the balancing of different interests. For instance, India's draft National Geospatial Policy notes that the sensitivity of geospatial data has to be judged by weighing the security or strategic considerations against the potential contribution to the country's socioeconomic development.[201]

Second, different stakeholders in the ecosystem tend to selectively rely on the perspectives that are most compatible with their commercial or ideological positions. Researchers at the Centre for Internet and Society mapped some of these broad trends based on their analysis of publicly available responses to the draft personal data bill put out by the Srikrishna Committee in 2018.[202] They found that, while most civil society groups opposed the blanket data localization norms, some academic and civil society actors saw them "as a remedy for 'data colonialism' by Western companies and governments."[203] Industry players and associations also expressed differing positions. Foreign companies like Google and Facebook were opposed to localization on the grounds of trade restrictions and compliance costs, while players like Reliance, PhonePe, and Paytm supported the move for furthering data sovereignty and the security of financial services.[204] Similarly, the views of different departments and agencies within the Indian government are shaped by their respective organizational priorities. Most of these differences in viewpoints are captured in the discussions that follow, though they are not necessarily disaggregated by stakeholder group.

Civil Liberties Perspective

The civil liberties perspective captures the link between data flows and personal liberty, autonomy, privacy and security, and the freedom of speech and expression. This is why regulations on cross-border flows often find a place in data privacy laws to ensure that the transfer of data from one jurisdiction to another does not diminish the protections guaranteed under domestic laws. In this respect, the Srikrishna Committee reasoned that a harmonious balance of mechanisms should be established for the protection of transferred data. This includes a mechanism for determining the adequacy of the transferee jurisdiction's laws, standard contractual clauses, and consent of the affected individuals.[205]

The fact that conditional transfers under the (since-withdrawn) DP Bill were supplemented by mandatory localization requirements, however, merits closer scrutiny from a civil liberties perspective. Autonomy, which is an important facet of privacy, demands that individuals should be empowered to make informed, independent decisions about the treatment of their personal data, including contractual decisions about the manner and location of data storage. But the Indian Supreme Court, while recognizing the fundamental right to privacy, clarified that the right remains subject to various reasonable restrictions. It can be overridden by the state for the pursuit of a legitimate aim that is backed by law and that satisfies the test of proportionality as laid down in *Justice K. S. Puttaswamy v. Union of India*, a 2018 Supreme Court judgment that upheld the constitutional right to privacy in India.[206] This case came up in the context of a challenge to the constitutional validity of India's biometric digital identity project, Aadhaar. Since then, the *Puttaswamy* tests of legality, legitimate aim, and proportionality have been applied by courts in several contexts.[207] Future courts may also be called upon to examine if the localization norms that India finally adopts would satisfy the *Puttaswamy* tests.

One component of such analysis should include assessing whether localization is the least intrusive means of achieving the state's legitimate social, economic, and strategic goals. This involves the balancing of multiple interests, including the impact on domestic and foreign surveillance. Easier access to data for domestic law enforcement agencies is one of the main goals of localization from the state's perspective. Yet localization without surveillance reforms would tilt the balance too far in favor of state access and against privacy rights. As discussed later, India's current laws allow domestic intelligence and law enforcement agencies fairly unfettered data access. The DP Bill's proposals on compelling certain categories of data to be stored or mirrored on Indian servers coupled with the exemptions suggested for state agencies would make data access even easier without corresponding safeguards for individuals.

Equally, the impact of localization on other freedoms, particularly the freedom of speech and expression, also needs to be considered. While the link between localization and free speech may not seem as apparent as in the case of privacy, localization can become a potent tool of censorship in the hands of the state.208 For instance, the Ministry of Information and Broadcasting recently announced the blocking of twenty-two YouTube channels under the new Intermediaries Guidelines Rules, 2021, on the grounds that they were spreading disinformation related to India.[209] Data localization combined with existing tools of censorship would only increase the likelihood of voluntary or forced adherence to such demands by regulated entities.[210]

Restricting foreign surveillance is another stated goal of data localization. In 2014, India's National Security Council suggested that "all email service providers" should be required "to host servers for their India operations in India."[211] This came up soon after the leaks by former U.S. contractor Edward Snowden brought to light the extent of foreign surveillance being carried out by the U.S. government and a few other states. While recognizing this as an important objective, the Srikrishna Committee also acknowledged that complete isolation from the internet in hopes of preventing foreign surveillance or meeting other security goals is not a feasible path for India.[212] The committee, therefore, used the threat of foreign surveillance as the basis for recommending the exclusive local processing (and storage) of a narrower set of information deemed to be critical data, a term left for the government to define.

Some of the other instruments and proposals discussed in table 1 also refer to privacy and security-related considerations. For instance, the Reserve Bank of India's Statement on Developmental and Regulatory Policies, which first announced the payments localization decision, spoke of maintaining the "safety and security of payment systems data . . . to reduce the risks from data breaches."[213] The Reserve Bank of India's local storage requirement for video know-your-customer data, which involves sensitive biometric information, also stems from the need to store data safely and securely.[214] Even the Gopalakrishnan Committee on nonpersonal data relies on the sensitivity of the underlying personal data as its basis for suggesting similar localization norms for nonpersonal data.[215] But an overall reading of the report makes it clear that the committee's recommendations focus primarily on the economic and strategic value of data with privacy featuring more as a collateral concern.

Government Functions Perspective

Three types of arguments are generally presented for restricting cross-border data flows to help the government perform its core functions. These are access to data for regulatory and law enforcement purposes, the preservation of national security interests, and data for informed policymaking.

The delays in accessing data stored in other countries for investigations and other law enforcement purposes features as a prominent justification for data localization in the Srikrishna Committee's report and that of the joint parliamentary committee.[216] Several of the sector-specific restrictions also focus on the need for data access to enable regulatory and supervisory monitoring. This is the case with the Reserve Bank of India's payment localization directive, which calls for "unfettered supervisory access" to data to "ensure better monitoring,"[217] and the Insurance Regulatory and Development Authority of India's localization mandate for policyholders' data in the name of regulatory access.[218] Another example is the Indian Computer Emergency Response Team's (CERT-In) mandate that certain organizations "enable logs of all their ICT systems and maintain them securely for a rolling period of 180 days" with the same records maintained within India's jurisdiction.[219]

The preservation of national security is another important justification in many of the Indian government's policy instruments. The Srikrishna Committee raised the issue of safeguarding the country's critical data from potential disruptions to the country's internet infrastructure, such as an attack on an undersea cable.[220] Beyond data protection, the localization mandate in some other instruments also stems from a national or systemic security perspective. For example, the localization provision in telecoms licenses "appears under the chapter on security . . . conditions, alongside other requirements relating to" national security and the public interest.[221] This suggests that the rationale for the restriction stems not just from the protection of subscribers' data but its broader implications for security interests. Similarly, the advisory issued by the CERT-In on the use of software as a service, which has been endorsed by the Securities and Exchange Board of India, aims to address the overall resilience of the financial sector's infrastructure to cyber attacks.[222]

Lastly, policy documents like the National Data Sharing and Accessibility Policy[223] and the recommendations on nonpersonal data by the Gopalakrishnan Committee mention the importance of data access for more informed decisionmaking by government agencies and the conducting of sovereign functions.[224] These documents do not draw a specific link between these objectives and data localization. Yet their mention of localization requirements suggests that it is seen as part of a general toolkit to achieve the policy's objectives.

Economics Perspective

The ability to extract the economic value of data that is generated in India factors prominently in data governance debates in the country. This is particularly true in the case of nonpersonal data, for which the committee's recommendations are premised on a need to correct the imbalance that enables large digital businesses to reap outsized economic benefits from their control over data.[225] In the case of personal

data, too, both the Srikrishna Committee and the joint parliamentary committee have highlighted the economic value of data in terms of spurring local innovation, creating employment opportunities, attracting investments, and strengthening India's domestic data center infrastructure.[226] However, while making these assertions, the reports do not seem to go the full distance in terms of demonstrating how data localization presents a logical path toward meeting each of these ends.

The claim about generating employment opportunities is precisely an example of the failure to demonstrate this link. The joint parliamentary committee's report points to the benefits of localization based on employment generation in the cloud storage market and the surrounding ecosystem. According to a table in the report, which is based on submissions to the committee, approximately 2,669 direct, indirect, and induced jobs can be expected to be created in India from the operation of large data centers to be established there by four leading companies—Amazon, Microsoft, Facebook, and Google.[227] While this is not an insignificant number, and although this figure is supported by other studies of job creation on account of data centers, it is still a modest figure given the size of the Indian labor market. It is estimated that the Indian IT sector alone accounts for about 5 million direct jobs.[228] The job estimates, therefore, do not demonstrate a strong case for mandatory localization on this basis.

The link between mandatory localization and data availability for boosting local innovation in artificial intelligence (AI) also merits closer scrutiny. Many have argued that the mere storage of data in India would not automatically make it accessible to researchers and businesses in the country.[229] Yet recent developments suggest that the state may use other tools like regulations on nonpersonal data to compel data sharing by private entities. The DP Bill proposed that India's central government would have the power to call upon any data fiduciary or data processor to provide any nonpersonal data for "better targeting of delivery of services or formulation of evidence-based policies."[230] The Gopalakrishnan Committee goes a step further in terms of broadening the purposes of such data requests and the entities that may make such requests. For instance, it would enable any organization registered in India to seek anonymized data about the sale of food items on an e-commerce platform or the starting time and duration of cab rides for research and innovation for the public good.[231] But even if such requirements were to come into effect, local storage of the data is not a prerequisite for operationalizing data sharing. Moreover, the current draft of the proposals does not compel data sharing for business and commercial uses.

Economic Impact of Local Data Storage

To be clear, these caveats are not meant to suggest that the creation of local data storage infrastructure would *not* yield economic benefits. In fact, a 2018 report commissioned by Facebook offers evidence to the contrary. According to the report, Facebook's four data centers "contributed a cumulative $5.8 billion in . . . [GDP] to the U.S. economy" between 2010 and 2016, an amount which translates to "$835 million per year."[232] A large portion of this amount (82 percent) was on account of the upfront capital investments for the construction of the data centers.[233] This supports the hypothesis that having data centers located in one's country generates significant economic benefits. The presence of such data centers may also generate efficiencies for local users of cloud services in the form of improved latency, meaning reduced time for the movement of data packets from source to destination.[234]

However, a distinction can be drawn here between situations where data centers emerge organically (influenced by geographic, economic, infrastructural, and political factors)[235] and scenarios in which this decision is coerced through restrictions on cross-border data flows. The latter scenario would yield an independent set of consequences in terms of compliance costs for businesses and costs for the overall economy that need to be factored into an assessment of the economic effects. For instance, stakeholders have noted that localization may deter some companies, particularly smaller businesses, from having a presence in India. Such requirements could also create barriers for local Indian entrepreneurs that rely on tools offered by other companies, which may not be in a position to rapidly satisfy these localization requirements.[236] In addition, the country's contribution to normalizing policies on data localization will also bear cost and compliance consequences for its own entrepreneurs and businesses operating abroad. Policy documents that propose localization have, however, either ignored the possibility of negative effects on digital trade or dismissed the concern as being one of compliance costs, which will be trumped by "the size and potential of the Indian market."[237] But a granular estimation of the costs and benefits of localization and an evaluation of alternative, less intrusive options has been largely missing from Indian policy discourse.[238]

Some research studies have tried to fill this gap by modeling how restrictions on data flows would affect India's trade prospects. For instance, researchers at the Indian Council for Research on International Economic Relations used "international internet bandwidth as a proxy for cross-border data flows" to estimate that a "1 percent decline in cross-border data flows [would] reduce [India's] volume of trade by $696.7 million."[239] In another study, Carnegie India's Anirudh Burman and Upasana Sharma deployed a multicriteria decisionmaking methodology to evaluate the suitability of different localization measures in the Indian context. They found that a requirement of local data storage coupled with the ability to process data globally "best meets the objectives of promoting economic growth."[240] However, the nature and extent of such benefits needs to be weighed against the overall costs of restricting cross-border data flows, which includes the social costs in terms of civil liberties.

Finally, many commentators have pointed to the disconnect between India's data center readiness and its ambitions for data localization, which is contingent upon the availability of the underlying infrastructure. The state of India's data center infrastructure has begun to change, however, with a surge in announcements of data center projects over the last few years.[241] A part of this can be attributed to the threat of localization in various policy documents, which can be viewed as a type of tactical bargaining strategy by policymakers. Companies might be strengthening their local data infrastructure to ward off the threat of mandatory localization or, in some cases, to be better equipped to reap the economic gains from it. But these developments are also accompanied by a more serious focus in government policies on promoting data centers. In 2020, the Ministry of Electronics and Information Technology introduced a draft National Policy on Data Centers that identified five strategies for growth in the sector. This included suggestions for improving the ease of doing business and creating a favorable ecosystem by focusing on the electricity supply and backhaul connectivity.[242] While the final policy has yet to be announced, earlier this year the Indian government announced the granting of infrastructure status to data centers, which will provide a boost to credit availability for the sector.[243]

The Geopolitics of India's Stance in International Discussions

In addition to the three domestically focused perspectives discussed in the previous section, India also holds a distinct strategic viewpoint on cross-border data flows. This position is reflected in the country's reservations about unhindered data flows that may jeopardize its domestic interests and an aversion to plurilateral arrangements that do not adequately reflect the voices and priorities of the developing world, a long-standing, central theme of India's foreign policy.

Globally, there are at least two major initiatives underway related to the free flow of data for commercial and business purposes. The first is the Osaka Track, which advocates data free flow with trust (DFFT), an initiative championed by former Japanese prime minister Abe Shinzo aimed at building an international arrangement on cross-border flows to foster innovation and economic growth.244 The second is the WTO's Joint Statement on Electronic Commerce, which includes the free flow of data.

Japan originally proposed the concept of DFFT at the World Economic Forum and later incorporated it into the declaration made by the G20 leaders in Osaka, Japan, in 2019. The declaration recognized the critical role of data as "an enabler of economic growth, development, and social well-being," highlighting both the benefits of cross-border flows and the challenges posed by them.245 In another meeting held on the sidelines of the G20 meeting, a majority of the members (nearly all of them—including China—with the exceptions of India, Indonesia, and South Africa) opted for the Osaka Track of discussions.246 This represented a commitment by the signatories to participate in "international policy discussions for harnessing the full potential of data."[247]

According to official statements, India has at least three main concerns with the Osaka Track. These include concerns about the country's ability to retain the freedom to make its own independent domestic policy decisions on digital trade and data, particularly on data protection and e-commerce; a lack of clarity around the concept of DFFT and the disconnect between uninhibited data flows and India's concerns of data access; and insufficient regard for the interests of developing countries in terms of equitable access to data and use of "data for development."[248] The last point connects with India's general stance on favoring a multilateral consensus on key digital trade issues, with equal representation for developing countries, instead of having these discussions in plurilateral forums.[249]

The Osaka Track signatories also affirmed their support for the Joint Statement on Electronic Commerce initiated at the WTO meeting held in Davos in 2019. With this statement, seventy-six member countries, a number that has now grown to eighty-six, declared that they intended to hold "WTO negotiations on trade-related aspects of e-commerce."[250] India remains fundamentally opposed to these negotiations, which it regards as a way of circumventing the principles of multilateralism and consensus-based decisionmaking.[251] New Delhi also believes that the current proposals on e-commerce would freeze an existing, unlevel playing field in favor of a few countries with globally dominant players.[252] According to a joint statement released by India and South Africa, a negotiation process on e-commerce should either be approved by consensus or take the form of bilateral or plurilateral trade agreements outside the WTO.[253] One of India's former ministers of commerce and industry has noted that this position also aligns with the views of other members of the African Group.[254]

Similar views have also surfaced in other venues that India participates in. In an informal BRICS meeting held in 2019, the members affirmed their commitment to safeguarding the role of data for development and reiterated the place of the WTO as the appropriate forum for such work.[255] India is also a member of the G77, a body that leverages the joint negotiating capacity of developing countries to pursue common economic interests.[256] The group's focus on inclusive and sustainable development has in the past led it to call out the substantial digital divides and data inequalities that exist in the current international system.[257]

Compared to its strong stance on e-commerce at the WTO, India has been more open to debating issues of cross-border data flows in bilateral and regional trade agreements.[258] In early 2022, India entered into a comprehensive economic partnership agreement with the United Arab Emirates (UAE), an agreement that has a chapter dedicated to digital trade. This includes a provision on cross-border data flows, which reads as follows:

> The Parties recognise the importance of the flow of information in facilitating trade, and acknowledge the importance of protecting personal data. As such, the Parties shall endeavour to promote electronic information flows across borders subject to their laws and regulatory frameworks.[259]

India's willingness to endorse this text can be attributed to at least three factors: the limits of its language (which only requires attempts to promote free data flows), the inclusion of a clear exception for domestic laws, and the fact that this chapter was not included within the scope of the agreement's dispute settlement provisions.[260] More recently, India also agreed to negotiate a digital trade chapter with Australia pursuant to the Australia-India Economic Cooperation and Trade Agreement that the two countries signed.[261] The negotiations on cross-border data flows will be particularly interesting given that Australia is one of the three countries leading the discussions on the Joint Initiative on Electronic Commerce.[262]

On the regional partnership front, despite reservations about the free data flow provision in the Regional Comprehensive Economic Partnership, India continued to participate in those negotiations.[263] While it ultimately did not sign the agreement, this decision was made primarily on account of tariff issues. The reasons the Indian government offered for its walkout did not include a reference to data flows.[264]

As things stand, India seems unlikely to support the WTO's Joint Initiative on Electronic Commerce though New Delhi appears to be more amenable to free flow discussions in bilateral and strategic partnerships. Further, the official statement made by the Indian minister of commerce after the Osaka G20 meeting noted that India did not join the track because its reservations were not accommodated. This does not, in theory, rule out future participation by India if the Osaka Track or a derivative of it evolves in a manner that can address some of New Delhi's key concerns about clarity on the meaning of DFFT, reserving domestic policy space, and acknowledging the role of data for development. India's 2023 stint holding the G20 presidency, during which it proposes to highlight the "issues and concerns of developing countries and emerging market economies,"[265] presents an opportunity to move in that direction although the intertwining between the Osaka Track and the Joint Statement on Electronic Commerce will remain problematic for India.

Challenges With Law Enforcement's Data Access

As more and more Indians use mobile phones and digital services, electronic evidence has become vital in many cases involving law enforcement. But India faces an odd dichotomy on the issue of data access for law enforcement. On the one hand, the current legal framework allows Indian intelligence and law enforcement agencies fairly broad powers of data access without adequate oversight and accountability.[266] This includes a general authorization in the country's criminal code for a police officer to call for any document or information required for investigating an offense.[267] A slightly higher degree of protection is provided in cases of intercepted communications, but in such instances, too, access for law enforcement is possible without prior or subsequent judicial review, transparency, or independent oversight.[268]

On the other hand, despite the overreaching powers available to Indian law enforcement agencies, data requests are sometimes not fulfilled due to the cross-border character of how data are processed and stored on the internet. The ability of law enforcement agencies to access data is shaped by a mix of factors. These include the laws of the country requesting data access (in this case, India), the business entity's home laws, and the rules applicable to the place(s) where the data are stored.[269] A statistic that often comes up is that eight of the top ten websites in India (in terms of web traffic) are U.S.-based sites that store and process large amounts of their data outside India.[270] This makes U.S. policies on data access, such as restrictions on third-party access to stored communications records, particularly relevant for India. In addition, access is also contingent on the nature of the data involved. For instance, basic subscriber information is generally easier to access than content data. Further, the technical design of end-to-end encrypted data, which is coded in a manner that can be deciphered only by the senders and receivers of the messages, makes it harder to access, even if the data were available locally.

Indian policymakers and law enforcement agencies have made various attempts to overcome frictions in seeking data access. Examples include the proposed carveouts for law enforcement and other government agencies under Sections 35 and 36 of the withdrawn DP Bill, the requirement placed on "social media intermediaries to trace the originator of a message or post if required by a court or competent authority,"[271] and a centralized monitoring system that gives authorized state agencies unhindered access to the information that flows through communication networks in India.[272] The centralized monitoring system, brought into effect through licensing conditions imposed on telecommunication service providers, requires those entities to connect their servers with the regional monitoring centers of the central system. Using this system, law enforcement agencies can directly carry out interception activities, subject to following the relevant processes under Indian law but without any involvement by the service providers.[273] Each of these initiatives poses significant concerns from a privacy and civil liberties perspective, leading to impending challenges before various courts to the legality and proportionality of some of these measures.[274]

This research builds on the author's previous work co-authored with Prateek Jha to focus only on actions targeted specifically at improving cross-border access by law enforcement.[275] At present, Indian law enforcement agencies have two main routes for seeking data that is stored abroad. The first is to directly approach the entity that holds the data in question by following processes enacted by different

companies for this purpose. For instance, Facebook (now Meta) reported that it received 40,300 user data requests from India between July and December 2020. The company provided some data in 52 percent of these cases.[276]

If the authorities fail to obtain the required information through this route or a direct request is otherwise not feasible, they can also send a formal request to the country that exercises jurisdiction over the data or the entity concerned. This can be done through cooperative mechanisms established under mutual legal assistance treaties (MLATs) or under a letters rogatory process, a formal request for assistance issued by an Indian court to a foreign court.[277] India currently has MLATs with forty-two countries.[278] A recent Indian parliamentary committee report revealed that, in 2021, India had 845 requests pending with various countries under these two processes.[279] Over 50 percent of these pending requests were with the United States, the UAE, the UK, Switzerland, Singapore, and Hong Kong.[280]

Several research studies and news reports have highlighted complexities and delays in the MLAT process. According to a 2015 *Economic Times* article, an internal survey by India's Central Bureau of Investigation found that on average an MLAT request took about forty months to be fulfilled.[281] However, the submissions made by various government ministries before the Parliamentary Committee on External Affairs curiously did not highlight MLAT delays as a particularly major concern. While the committee itself raised the alarm about the 845 pending requests, its report does not contain any details about how long these requests had been pending or the reasons for these delays.[282] The committee directed the Ministry of External Affairs to constitute a task force to look into the matter.

The relevant academic literature suggests that such requests can lead to delayed responses or refusals not only due to lengthy procedures in the corresponding country but also due to incomplete or poorly drafted requests. Furthermore, such requests may also tend to prompt refusals if they are raised on matters that do not qualify for such assistance, such as *de minimis* requests, which are deemed trivial or disproportionate in nature.[283]

Actions taken to improve the MLAT process include joint efforts at training and capacity building, including collaboration between India's Central Bureau of Investigation and the U.S. Federal Bureau of Investigation.[284] In 2019, India's Ministry of Home Affairs also revised its comprehensive guidelines on this issue laying down step-by-step procedures and the recommended form and content of such information requests.[285] Moreover, as discussed in the previous section, both the Srikrishna Committee and the joint parliamentary committee identified faster data access for law enforcement agencies as grounds for supporting data localization. Commentators, however, have questioned the use of localization as a solution to this problem, as local storage would neither override conflict-of-laws problems, including restrictions on data sharing imposed by a multinational corporation's home jurisdiction, nor enable access to encrypted data.[286]

Further, when seeking alternatives to promote data access for law enforcement, there is a need to look to international instruments like the Budapest Convention, which gives member states the option of direct access to data under certain circumstances. India is not a signatory to the Budapest Convention,

"which is the only binding international instrument" on cybersecurity at present.[287] The reason for India's position is that New Delhi regards the Budapest Convention as a regional European initiative that is not sufficiently broad-based to be internationally acceptable.[288] This stance led India to support a 2019 UN General Assembly resolution introduced by Russia to work toward an international convention on countering the use of ICT for criminal purposes. This initiative, however, has been criticized for its failure to balance the interests of law enforcement and respect for fundamental human rights, a balance that many argue is better achieved under the Budapest Convention.[289] Besides concerns about the proper balancing of such interests, progress on this resolution could also be negatively affected by the crisis created due to Russia's invasion of Ukraine.

The report of the Parliamentary Committee on External Affairs chaired by P. P. Malhotra, the same member of parliament who chaired the joint parliamentary committee on data protection, made some interesting observations on this issue. Without specifically naming the Budapest Convention, the committee urged the Indian government to "secure the cooperation of countries with established multilateral and regional instruments of cooperation on cyber security protocols."[290] The committee also observed that, rather than pushing for localization "which is proving to be impossible in [the] near future," the government should strengthen its cybersecurity laws and capabilities for now and then gradually proceed in the direction of data localization as a means of addressing power asymmetries in cyberspace.[291] In its submissions to the committee, the Ministry of External Affairs noted that the government would examine the Budapest Convention more closely after deliberations on the DP Bill conclude.[292] With the withdrawal of the DP Bill, such an examination is likely to be further delayed.

Three main observations can be drawn from these discussions. First, the issue of efficiency in relation to law enforcement's data access is intrinsically linked to the broader need for safeguards and accountability in how law enforcement agencies use such data. Trying to solve one problem without addressing the other would lead to grossly suboptimal solutions from a human rights perspective. Second, the link between localization and access to cross-border data is not as simplistic or obvious as it is sometimes made out to be. Third, while India may continue to engage with the UN resolution process on developing a cybersecurity convention, the country needs to more seriously consider participating in existing mechanisms such as the Budapest Convention, which do more to respect rights and offer immediate solutions.

A Way Forward

The recent policy discourse in India reflects the country's growing assertions of technological self-reliance and sovereignty in data governance. The same logic also extends to other avenues like the promotion of homegrown application programming interface solutions, the focus on domestic startups and unicorns, and the stricter regulation of online intermediaries. On a macro-level, these developments signal a desire to shift India's position from being just a large digital user to having a more controlling stake in shaping digital outcomes. The country's position on cross-border data flows must be seen in the context of this larger debate.

India's unique position on cross-border data flows is shaped by a mix of domestic priorities and the multiple identities that it straddles on the international stage. This analysis began by discussing the instruments and arguments that are driving India's policies on cross-border data flows. Current restrictions on data flows are concentrated in financial services, telecommunications and broadcasting, corporate and compliance records, and government data. In addition, India has had a vibrant policy debate over the last few years on the localization of personal data, and, more recently, nonpersonal data. This is indicative of a shift toward more wide-ranging and cross-sectoral localization norms.

This analysis examined the justifications offered for these moves through the lens of various motivations, including preserving privacy and civil liberties, performing state functions, developing the local economy, and addressing geopolitical and strategic considerations. It finds that the case for restrictions on data flows on these grounds is generally based on assertions, not robust evidence. When such justifications are supplied, policy documents rarely demonstrate how data localization presents a logical path toward meeting the desired ends or how the perceived benefits stack up against the social and economic costs of localization. The committee reports on data protection do a better job of engaging with these issues compared to the sectoral localization mandates. But even in the committee's report, the link between local data storage and goals like promoting local AI innovation or ease of access by law enforcement agencies for all types of data has not been adequately demonstrated.

The practice of offering multiple explanations or claimed advantages for the same policy poses another problem. This approach misses the fact that the varied objectives behind a policy move could often conflict with one another. The tussle between the goals of easier data access for surveillance and law enforcement purposes and the risks of curtailing privacy and other civil liberties is a case in point. Similarly, broad surveillance powers for the Indian government could deter foreign firms from setting up cloud servers in India or utilizing Indian ICT service providers, and these consequences would conflict with the economic goal of creating a vibrant data market in the country. For instance, ExpressVPN recently became the first virtual private network provider to remove its servers from India. It made this decision in response to the intrusive data requirements imposed by the government's new CERT-In directive on cybersecurity.[293] In addition, having such a multiplicity of objectives can blur accountability by making it possible for agencies to pick and choose varying explanations for their actions in different contexts. This issue is compounded by the lack of tools for systematically measuring the consequences and effects of such policy moves.

In debates on international data flows, meanwhile, India's positions are being shaped by interactions between the country's stated priorities and its assertion of its identity as a developing country. India has been a vocal critic of unhindered free flow of data, which the Indian government believes fails to account for emerging economies' developmental interests. This stance led New Delhi to opt out of the G20's Osaka Track and the Joint Initiative on Electronic Commerce, although the Indian government appears to be more open to discussing data flows in bilateral and regional trade agreements.

While there are several country-specific nuances at play, global differences on the free flow of data can crudely divide countries into two categories. Members of the first group prioritize the idea of data for innovation and economic growth, viewing growing restrictions on data flows as a barrier to trade. In

contrast, the second group focuses on the role of "data for development," treating data as a form of national wealth that needs to be safeguarded from external exploitation and made available for domestic requirements.[294] Reaching a reconciled understanding between these positions, while difficult, is possible provided that all viewpoints are brought to the table. India will have the opportunity to take a lead in facilitating such an open and nonbinding discussion during its upcoming stint holding the G20 presidency. However, this would be feasible only if such discussions can take place outside of the current design of the Osaka Track since participation in the track indicates that a country endorses the WTO Joint Statement, which India strongly opposes.

On the issue of data access for law enforcement, this analysis highlights an odd dichotomy whereby Indian law enforcement agencies on the one hand enjoy wide, unchecked legal powers of data access but, on the other hand, conflict-of-laws prevent them from freely accessing data under the control of foreign corporations. Any move to reduce frictions in access to foreign data, whether through localization or international agreements for direct data access, must therefore be accompanied by domestic surveillance reforms. Failing this, easier data access would only exacerbate the privacy and human rights concerns in India's current surveillance framework. Keeping in mind this overarching recommendation, the following moves can be considered for improving the existing systems of data access for law enforcement purposes without coercive localization.

First, these practices can be made more efficient and consistent if the government publishes the formats and protocols for sending direct information requests to service providers, similar to the guidelines for MLAT requests. This may be accompanied by the creation of a streamlined technical architecture to monitor the authentication and flow of such data requests in a standardized and secure format.[295]

Second, the Indian government should initiate bilateral dialogues with countries like the United States, the UK, and Australia that are among India's key digital partners. The purpose of such dialogues would be to tangibly improve the mutual assistance process. This may include joint training programs, resource and time commitments for the handling of data access requests from abroad, and other capacity-building measures. Drawing on the recommendations of the Parliamentary Committee on External Affairs, India would also benefit from the creation of a task force to evaluate the implementation of its MLAT guidelines and identify the duration of and reasons for undue delays and rejected requests.

Third, the Indian government ought to create a multistakeholder task force to evaluate the pros and cons of international agreements on direct data access and formulate India's position on this issue.[296] This could be the same body as the one referred to above or a different one, the critical consideration being to ensure representation from a "diverse group of stakeholders, including representatives from different government departments, the private sector, civil society organizations, and experts in international law."[297] Further, while India may continue to engage with the UN resolution process on developing a cybersecurity convention, it needs to more seriously consider participating in existing mechanisms like the Budapest Convention.

In conclusion, effective and consistent data policies that enable Indians to fully engage in the global economy will benefit Indian users and the businesses serving them as well as the country's burgeoning start-up ecosystem, with an eye toward global markets. India enjoys a unique position as an emerging digital power, a strategic digital partner to several advanced economies, and a country that shares its developmental priorities with large parts of the developing world. Its ability to reach a nuanced response on the issue of cross-border data flows is therefore important not just for achieving its own economic, strategic, and human rights ends but also in terms of the possibility of bridging the global divide on governing cross-border data flows.

The author's views represent her own independent analysis and should not be understood as representing the official policy of any government.

Table 1. India's Current and Proposed Restrictions on Cross-border Data Flows

Data Type	Agency	Instrument	Requirement	Status
Financial Sector Data				
Insurance policyholder records	Insurance Regulatory and Development Authority of India	Outsourcing of Activities by Indian Insurers Regulations, 2017[298]	"In cases where Insurer outsources to the service providers outside India, the Insurers shall ensure . . . compliance with respective local regulations [and that] . . . regulatory access and oversight by the Authority [are not impeded]. All original policyholder records continue to be maintained in India."[299]	In effect
Payments data	Reserve Bank of India	Directive on Storage of Payment System data, 2018[300] A related webpage with frequently asked questions (FAQs) on storage of payment system data[301]	All data related to payment transactions is to be "stored in a system only in India."[302] The FAQs webpage clarified that data can be processed abroad but has to be deleted within twenty-four hours and stored only in India. There is an exception for "data pertaining to the foreign leg of [a cross-border] transaction [that] can be stored outside the country."[303]	In effect
Video know-your-customer verification data	Reserve Bank of India	Amendment to the Master Direction on Know Your Customer, 2021[304]	Entire data and recordings of the video customer identification procedure are to be stored in systems located in India.	In effect
Communications and Broadcasting Data				
Telecoms subscriber data	Department of Telecommunications	Unified License Agreement entered into between the Department of Telecommunications and telecommunication service providers[305]	Restrictions on transferring any "accounting information relating to [a] subscriber" or "user information" to "any person/ place outside India."[306] Exception for transfers made for international roaming and billing purposes.	In effect
Broadcasting subscriber data	Ministry of Commerce and Industry's Department for Promotion of Industry and Internal Trade	Consolidated Foreign Direct Investment Policy, 2020[307]	Foreign direct investment is subject to the condition that "the company shall not transfer . . . subscribers' databases to any person/place outside India unless permitted by relevant law."[308]	In effect

Corporate and Compliance Data				
Books of companies' accounts	Ministry of Corporate Affairs	Companies (Accounts) Rules, 2014[309]	"Back-up of the books of account and other books and papers of the company maintained in electronic mode . . . shall be kept in servers physically located in India."[310]	In effect
Risk and compliance data of financial institutions	Securities and Exchange Board of India based on an advisory by CERT-In	Advisory for Financial Sector Organizations Regarding Software as a Service (SaaS) Based Solutions[311]	Financial institutions utilizing software as a service must keep critical data relating to risk, audits, and compliance within the legal boundary of India.	In effect
Government Data				
Public records	Parliament, National Archives of India, and the Ministry of Culture	Public Records Act, 1993[312]	Prohibits anyone from "tak[ing] or caus[ing] to be taken out of India any public records without the prior approval of the central government." Approval is not needed if the document is "sent out of India for any official purpose."[313]	In effect
Cloud storage of government data	Ministry of Electronics and Information Technology	Guidelines for Government Departments on Contractual Terms Related to Cloud Services[314]	Empanelment conditions for providing cloud services to the government require that "data center facilities and the physical and virtual hardware should be located within India."[315]	In effect
Shareable data held by the Indian government	Department of Science and Technology	National Data Sharing and Accessibility Policy, 2012[316]	The policy's implementation guidelines state that the open government data platform is to be managed and hosted at the National Data Centre of the National Informatics Centre.	In effect
Cross-sectoral Application				
Logs of all ICT systems	Indian Computer Emergency Response Team (CERT-In)	Directions under Subsection (6) of Section 70B of the Information Technology Act, 2000[317]	"All service providers, intermediaries, data centres, body corporate and government organisations" need to keep ICT system records in India "for a rolling period of 180 days."[318]	In effect (An extension on some aspects has been granted until September 2022)[319]
Sensitive personal data	Ministry of Electronics and Information Technology	Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[320]	Transfer of data is allowed only "if it is necessary for the performance of [a] lawful contract" or with the person's consent.[321]	In effect

Personal data, sensitive personal data, and critical data	Ministry of Electronics and Information Technology Joint parliamentary committee on data protection	Personal Data Protection Bill, 2019 and DP Bill (2021)[322]	Mirroring requirement for all sensitive personal data and critical data, which has to be stored and processed only in India.	Proposed by the Srikrishna Committee (The DP Bill has now been withdrawn with plans to introduce a new draft.)
Nonpersonal data derived from personal data	Gopalakrishnan Committee	Report by the Committee of Experts on Nonpersonal Data Governance Framework, 2020[323]	Nonpersonal data "shall inherit the sensitivity of the underlying personal data for storage requirements as specified in the [data protection bill]."[324]	Proposed
Other Proposals				
Healthcare data	Ministry of Health and Family Welfare	Digital Information Security in Healthcare Act, 2018[325]	Proposed the creation of a National Electronic Health Authority that would have the power to enact protocols for the exchange of digital healthcare data with other countries.[326] No specific localization requirement.	Proposed (but the draft law has been abandoned)
E-pharmacy data	Ministry of Health and Family Welfare	Draft Drugs and Cosmetics (Amendment) Rules, 2018[327]	"The E-pharmacy portal shall be established in India . . . and shall keep the data generated localised." Data are not to be "sent or stored . . . outside . . . India."[328]	Proposed
E-commerce data	Ministry of Commerce and Industry's Department for Promotion of Industry and Internal Trade	Draft National e-Commerce Policy, 2019[329]	Restrictions on flow of "data collected by [Internet of Things] devices installed in public places . . . [and from] various sources including e-commerce platforms, social media, search engines etc."[330]	Proposed (but the localization provisions have reportedly been abandoned)
Geospatial data	Department of Science and Technology	Draft National Geospatial Policy, 2021[331]	The draft notes that the government does not intend to restrict the export of maps and geospatial data subject to the threshold values and negative lists to be specified by the department.[332]	Proposed

CHAPTER 4

Korea's Path to Best Practices for Cross-Border Data Flows

KYUNG SIN "KS" PARK

As demand for digital services grows, some proposals for data localization, often motivated by governments' desire to protect citizens' privacy or to enable law enforcement surveillance, could hinder the free flow of data. In South Korea (hereafter Korea), calls for localization have become more frequent and more forceful in recent years, culminating in the 2018 server localization bill, which requires all online service providers above a certain size to place their servers within the country so as to provide "stable services."[333]

Yet there are other approaches, including the assimilation of international arrangements and instruments, that could enable Korean policymakers to realize their policy goals *without* mandating such data localization. For instance, if their goal is to facilitate law enforcement access to citizens' data that may lie outside the jurisdiction of the Korean government, the Budapest Convention may provide an alternative to the time-consuming mutual legal aid treaty (MLAT) processes that require law enforcement agencies to request help from their foreign counterparts. Similarly, if addressing concerns about citizens' privacy is the policy goal, then the European Union's (EU) General Data Protection Regulation's (GDPR) adequacy process or the certification process of the Asia-Pacific Economic Cooperation (APEC) forum's Cross-Border Privacy Rules may provide the needed level of protection, no matter where the data may be stored and processed.[334] If the goal is to counter the market dominance of foreign online services, then any measures will need to be assessed in light of World Trade Organization (WTO) trade rules that deal with state parties' mercantilist aspirations to nurture domestic industries. Although such legal analysis on trade may not assuage calls to prevent "digital colonialism,"[335] the trade rules are a constraint that could bind policymakers in designing sustainable ways to meet their goals without requiring data localization.

This analysis assesses Korea's data localization discourse, examines the different justifications for data localization initiatives, and explores a range of legal instruments that might help address those policy concerns. It first explores Korea's own data localization initiatives. It then dives deeply into the Budapest Convention and its implications for Seoul, before turning to questions of competing against foreign dominant players according to the trade regimes and international approaches that Korean policy can and should assimilate. Whichever of these international alternatives to localization is adopted, a key concern is that such alternatives address what Korean commentators call regulatory "reverse discrimination," an issue originating from the thicket of unusual and specific online service regulations often unique to the country.[336] In addition, the prospect of the Budapest Convention serving as an alternative to data localization is resisted by locals due to their desire for more privacy by having the option of communicating through foreign platforms that are supposedly more compliant with human rights. This aspect of Korea's localization discourse calls for a concerted focus on human rights.

The Context of Korea's Data Localization

Data localization measures are one of the many ways governments try to assert digital sovereignty or strategic autonomy (however those terms are defined). Anupam Chander of the Georgetown University Law School and Haochen Sun of the University of Hong Kong Faculty of Law attribute such efforts to governments' desires to protect their citizens, build their domestic digital economies, and control their own citizens.[337]

But one challenge with this classification is that it is difficult to distinguish between measures designed for protection and those designed for control. For instance, if a nation requires all content providers to locate their main servers domestically so that the police or other censorship bodies can directly order content to be blocked, their stated motivation is to control *bad* actors who upload dangerous online content and protect the public who may suffer harm. One example is China. But given how its state-centric approaches to cyberspace are derived from Communist ideology, it can be difficult to distinguish the Chinese government's measures of controlling the public from its efforts to protect the public.[338] In addition to China's Cybersecurity Law (enacted in 2017), the country has a firewall that filters internet traffic into and out of the country, ostensibly for the purpose of protecting Chinese people's data, but this approach also enables internal surveillance and censorship.[339] Instead of distinguishing protection from control, both kinds of measures can be motivated by a desire for sovereign control of data.

The Korean government also seeks sovereign control of data, but Seoul's justification varies depending on the type of data. Much like the EU, Korea has strict data protection laws for personally identifiable information. These laws, like the adequacy scheme in the EU's GDPR, have a single aim—to protect citizens' data, or equivalently data protection—but they do so without requiring that personally identifiable information remain within the reach of domestic surveillance and censorship. One side effect of these laws is that they limit governments' power over citizens, the opposite of enhancing sovereign control of data.

Moreover, some data localization rules are not for the purpose of protecting personal data. For instance, Korea still prohibits map data of precision above a certain level from physically leaving the country to protect national security.[340] Other laws, such as India's requirement that financial data remain within the country, are meant to ensure effective regulatory oversight.

Ultimately, Korean arguments for data localization can be grouped by the following five motivations: national security, sovereign control of data, data protection, fair taxation, and fair competition.

National Security

After U.S. national security contractor Edward Snowden revealed that various domestic U.S. government surveillance programs had an extraterritorial impact because much of the world's internet traffic goes through servers located in the United States, several countries, including Brazil and Germany, sought to keep their domestic online traffic safely out of the reach of the American surveillance program. After the Snowden revelations, Germany's data protection authorities also requested that Deutsche Telekom keep internet traffic within Germany as much as possible and proposed creating a Bundescloud, a cloud infrastructure for all data held by German government agencies (to be established by 2022). The German authorities further proposed a data network restricted only to EU users.[341] Ironically, had such proposals been implemented, German users would today be more vulnerable to surveillance by German government agencies. Brazil attempted something similar. Its proposed data localization law was a clear response to concerns about foreign surveillance, but in the final version of the country's Civil Rights Framework for the Internet (better known as Marco Civil da Internet), the data localization requirements were removed.[342]

Sovereign Control of Data

Independently, Russia and China have been on course to enhance sovereign control over their citizens' data for purposes of both censorship and surveillance. While these data localization laws reflect a desire for digital sovereignty, it is clear that both regimes (and several governments in the Middle East and elsewhere) view freedom of speech and truly private, encrypted communications as threats to national and regime security. In other countries, data localization is justified by a desire to harness the utility of locally generated, nonpersonal data for a range of business and governmental purposes.

Data Protection

Meanwhile, GDPR aims to protect EU citizens' privacy by ensuring that their data are not transferred into jurisdictions with what are deemed inadequate levels of data protection. But defining what is considered adequate has proven challenging, as evidenced by the years of negotiations over the U.S.-EU Safe Harbor Framework and the EU-U.S. Privacy Shield Framework, which have governed data transfers between the United States and the EU. Unlike other types of data localization measures, which are designed to meet a government's needs, GDPR (and similar Korean laws governing personally identifiable

information) protect and empower citizens. These laws do not block data transfers if data subjects give consent, regardless of the adequacy level of the destination jurisdiction. The goal is self-determination rather than state control.

Fair Taxation

Many governments want companies to host their content and services on domestic servers to ensure they can tax foreign content providers that otherwise could make money there without establishing a physical presence.[343] But taxing remote servers is against general rules of taxation, so foreign internet companies are taxed at a much lower rate than domestic companies. While the EU Commission has decided to address this discrepancy by bending tax rules (through tax base erosion and profit shifting),[344] several Southeast Asian countries have required that relevant servers remain within their borders.[345]

Fair Competition

Martin Schulz, who formerly was president of the European Parliament, warned that the market power of "digital giants" poses not just economic problems but also social problems.[346] GDPR's data portability provisions were an attempt to counter such dominance by allowing internet users to more easily shift from one online service to another when the EU's Data Retention Directive was declared invalid by the Court of Justice of the EU in 2014.[347] Other European politicians have been more direct and vocal in their calls to protect and promote domestic companies.[348] It is not clear, however, whether GDPR's adequacy scheme, the only comprehensive data localization for Europe, is an appropriate or effective vehicle for such data mercantilism.

Korea's Data Localization Discourse

Korea's debate over data localization is unusual because of its central focus on fair competition, or to be more specific, the eradication of discrimination against domestic online services. This trend is evident from the ubiquity of the term "reverse discrimination" in news articles reporting on the country's 2018 server localization bill.[349] Similar sentiments have been heard in India and a few other countries where domestic companies have a sizable share of the local market for online services.[350]

Yet Korea's data localization discourse on fair competition is more heated than elsewhere because of the long list of parochial regulations applicable only to Korean online services ranging from its internet real-name law, game shutdown laws, upload filter requirements, and more.

The underlying idea in Korean discourse is that these regulations place domestic providers at a disadvantage compared to foreign providers because the regulations apply only to providers that are located domestically, so (the thinking goes) forcing foreign providers to localize by placing servers within Korean territory will ensure equality of regulation and hence fair competition. However, this approach begs the question of whether international economic law allows mandatory data localization rules as a tool for fostering such claims of fair competition. What is more, if the answer to that question is no, then it begs a secondary

question of what the best practices are for achieving fair competition. In addition, as is the case in Brazil, there are few (if any) calls in Korea for data localization stemming from law enforcement's inability to access overseas data concerning domestic persons in Korea. In this respect, Korea is very different from India, where law enforcement access is a primary concern.

In Korea, both of these themes, fair competition and sovereign control of data, have been advanced as main justifications for data localization, but the country's current approaches to data localization do not reflect best practices for achieving these goals. Firstly, accession to the Budapest Convention would protect a workable version of data sovereignty but would obviate the need for data localization. Secondly, the WTO's trade rules, which Korea has agreed to, prohibit data localization motivated by desires to protect domestic providers. However, that is not the end of the story. The sections below explore these themes through legal analysis and consider how the general public might view such legal analysis.

The Budapest Convention and Extraterritorial Data Access for Law Enforcement

Korea can and should look to the Budapest Convention as an alternative way to secure its interests.

The Budapest Convention

The Budapest Convention facilitates information sharing among law enforcement agencies in different countries, including nearly all of the forty-six member states of the Council of Europe and some nonmember states.[351] The convention is the first binding multinational treaty to comprehensively address not only cyber crimes but also the gathering of electronic evidence of noncyber-related criminal activity.

The Council of Europe's first work on computer-related crime began in the 1970s.[352] This led to the 1989 recommendations for national legislatures and the "Report on Computer-Related Crime" for developing the necessary substantive criminal law to deter electronic crimes.[353] In addition, a recommendation on criminal procedural laws dealing with information technology was adopted in 1995.[354] These recommendations led to a draft of the Convention on Cybercrime (another name for the Budapest Convention), and the convention was opened for signatures at a November 2001 conference in Budapest, Hungary. Since then, the Protocol and Guidance Notes were created to support the convention's implementation.[355]

The Budapest Convention was initially intended to harmonize substantive criminal laws concerning computer systems and data, namely for cyber crimes; provide national criminal justice authorities with the necessary means for investigating and prosecuting such criminal offenses; and to establish an effective mechanism of international cooperation in combating these offenses. Chapter 2 of the convention specifies the following nine offenses: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offenses related to child pornography, and offenses involving infringements of copyright and related rights.

What is important for Korea is that this same chapter of the convention also provides for investigative means, including expedited preservation of stored computer data, production orders, search and seizure of stored computer data, and real-time collection of computer data. Moreover, these provisions apply to any other criminal offenses committed by means of a computer system and finally to the collection of evidence in electronic form of any criminal offense. In addition, Chapter 3 of the convention on international cooperation contains general principles and procedures relating to extradition and to traditional and mutual legal assistance for computer-related crimes.

Korea's Position on the Budapest Convention

Many Korean commentators have called for the country's accession to the convention, citing the need for cross-border cooperation on fighting cyber crime, which spans national borders.[356] Existing bilateral mutual aid treaties between Korea and other countries enable cooperation between law enforcement agencies, but this can be a slow process and varies from country to country.[357] These problems were documented in a recent and unprecedented empirical study of the efficacy of the Budapest Convention in facilitating cross-border cyber crime investigations.[358] If Seoul were to sign on to the convention, it would not replace MLATs among the countries that already have such a treaty with Korea, but such a move would help facilitate such collaboration.

However, many Korean privacy advocates are concerned that the convention (in Article 20) mandates real-time collection of metadata.[359] Still, the current Korean wiretapping law, the Protection of Communications Secrecy Act, regulates metadata acquisition in Article 13, even though technically the textual scope of the law is limited to "data confirming that communication has taken place," which does not include real-time metadata acquisition.[360] Indeed, for years, real-time metadata acquisition has taken place under these existing provisions. As a result, in 2018, Korea's Constitutional Court commented on the lax standard in a ruling related to real-time location tracking.[361] In response to the decision, the law was amended in a way that implied that metadata acquisition by definition includes real-time acquisition.[362] Overall, it seems that these privacy concerns that have repeatedly stymied efforts to get Korea to sign onto the convention can be addressed.

Other Korean skeptics point out that accession would necessitate several legislative changes to meet the convention's harmonizing requirement. Article 16 of the convention (on the expedited preservation of stored computer data) also lacks an explicit counterpart under Korean law.[363] However, the country's existing search-and-seizure system could be easily adapted to meet the convention's requirements.[364] Article 17 (on expedited preservation and partial disclosure of traffic data), designed to clarify Article 16's scope over multiple service providers involved in one instance of communication and allow expedited disclosure of each service provider's traffic data to identify other service providers involved, also lacks an explicit counterpart in Korean law, but, again, it seems that the country's existing search-and-seizure measures could also be adapted for this purpose.[365]

Some critics point to Article 18 (on production orders), which requires an alternative to Article 19 (on search and seizure of stored computer data) that would allow service providers a legal basis to voluntarily cooperate on such government requests.[366] The need for this alternative arises from the legal difference between a warrant, which merely permits law enforcement to obtain access, and an (affirmative) order that compels private parties to produce the data. However, the Protection of Communications Secrets Act is already crafted in light of service providers' duty to cooperate and therefore already provides the legal structure necessary for a production order to be issued instead of a warrant.[367]

Others point to the portion of Article 18 on production orders as applied to "subscriber information," a point of contention that has created many privacy-related controversies in Korea because subscriber data is accessible without a warrant in the country under the Telecommunication Business Act (Article 83, Paragraph 3).[368] However, the convention simply requires the existence of a production order and is silent on whether subscriber data can be obtained without a warrant. Also, due to the aforementioned controversies, Korean courts have already used search-and-seizure warrants to authorize law enforcement access to subscriber information since early 2013.[369] It is true that Korean law needs be changed to create a system for production orders, as opposed to one for search-and-seizure warrants. The previously mentioned orders under the Protection of Communications Secrets Act apply only to metadata related to specific communications and therefore will not cover subscriber information, which is often not related to specific communications.

Another consideration is that Article 19, Paragraph 2 of the Budapest Convention (on search and seizure of stored computer data) requires an intraterritorial remote search-and-seizure procedure. However, the Korean Supreme Court already has recognized the validity of such remote search and seizure even for extraterritorial access.[370] Although the remote search and seizure in that case was executed by obtaining the access credentials directly from the owner of the email account, instead of executing the warrant on the service provider, on whom it could not be executed anyway because the company did not reside in Korea, the ruling in this case would easily justify such remote search and seizure through a warrant executed upon the service provider within the country. Some still argue that remote search and seizure must be authorized explicitly by the statute.[371]

Besides privacy issues, some critics are concerned about the increased compliance costs on digital intermediaries.[372] Others are concerned that making domestic surveillance easier could increase the risk of security breaches arising out of foreign actors' access to domestic data.[373] Article 6 of the convention (on the misuse of devices) requires criminalizing the production and sale of devices, programs, and credentials for the purpose of committing the data-related offenses defined in the convention; there are no similar provisions in Korean law. Meanwhile, Article 12 (on corporate liability) establishes dual criminality including for both perpetrators and the corporations hiring them, and Korean law lacks such provisions.[374]

In sum, the statutory hurdles to Korean accession to the Budapest Convention do not seem insurmountable. The necessary changes could be made to existing Korean law by making minor revisions or interpreting statutes more broadly. However, resistance to such a move stems from the possibility of erosions of freedom from surveillance or simply privacy concerns.

What Korean Critics Miss

Overall, while it seems that legal hurdles to or privacy concerns about the Budapest Convention can be overcome relatively easily, support for Korea's data localization rules or for the country's accession to the convention will depend very much on public opinion regarding domestic surveillance, rather than on the political will of law enforcement leaders.

Korean law enforcement has not been vocal in its support for accession to the Budapest Convention. Not until 2020 did the National Police Agency commission its first study on the subject, and this study aimed not to persuade the government to accede but only to find out what domestic laws would need to be changed in the wake of accession.[375] It was feminist organizations in Korean civil society that first advocated for the country's accession to facilitate investigations of digital sex crimes.[376]

One reason there has been so little progress toward accession so far may be that the Korean police often rely on confessions as much as on evidence (whether physical or digital) when conducting investigations. The value of surveillance for Korean law enforcement has been more for identifying suspects than for proving guilt. For these reasons, the number of interceptions conducted by general law enforcement (as opposed to the National Intelligence Service with its mandate to conduct externally focused intelligence activities) has been very small.[377] The mass surveillance type of data access, designed to identify suspects from large customer databases, has been much more intensive in Korea. The number of Korean "phone numbers, email addresses, and other accounts" affected by metadata acquisition has reached 37 million per year, a significant figure in a country of 50 million people.[378] Of course, metadata acquisition was originally designed to prove guilt of a preidentified suspect. In Korea, that metadata acquisition takes place mostly for the purpose of finding suspects, just as the U.S. National Security Agency did after the 9/11 terrorist attacks (as Snowden revealed). What complements metadata acquisition has been the warrantless acquisition of subscriber information, through which Korean authorities could scan huge volumes of metadata to find a few suspects.[379] In any case, Korean law enforcement has not actively sought out the deep extraterritorial surveillance capabilities afforded by the convention. Notably, these high volumes of surveillance have raised Korean people's sensitivity about privacy or freedom from sovereign surveillance.

Finally, the Korean public clearly prefer to have foreign communications platforms available for them so they can store data beyond the reach of domestic prosecutors. Whenever the media reports on the overreaching surveillance practices of Korean law enforcement, there has been a massive "cyber exodus," a migration of users of online services from Korean providers to foreign ones.[380] Ironically, the Budapest Convention itself may not be welcomed by Korean citizens who want offshore locations for storing their data lest their data would be more easily available to Korean authorities under the convention. Having said that, these savvy users would prefer to have no data localization measures so they can move their data where they please, and they also would prefer to not have a convention that makes it easier for Korean law enforcement to retrieve their data from a foreign service provider. So the very reasons for opposition to the Budapest Convention have operated behind the scenes to practically preempt calls in Korea for sovereignty-based localization: the reasons explaining Korean law enforcement's disinterest in the convention also easily explain their reasons for disinterest in data localization.

That said, there really is no human rights norm, international or municipal, stating that people should be guaranteed access to communication platforms beyond the reach of domestic prosecutors, though the availability of such platforms does reduce the risk of surveillance. The push for data localization can originate from different motives, not just from sovereign control of data. It is possible that the threat landscape could change in Korea (as it did in the United States after the 9/11 attacks) causing national security agencies and law enforcement agencies to want better access to data located overseas. If that happens, Korean people who choose overseas communication platforms will be better off with the convention than they would be if their data was stored domestically.

Promoting Fair Competition Under International Economic Law

Korea also has another path to better practices when it comes to facilitating fair competition for Korean companies vis-à-vis foreign rivals in terms of regulations applicable to internet content providers.

Korea-Specific Regulations of Online Services

There are several Korean laws that put local providers of online services at a disadvantage compared to foreign providers used by Korean consumers. For one, under the Telecommunication Business Act,[381] all domestic providers of online services with more capital than the equivalent of about $100,000 must maintain registration as a "value-added service provider."[382] Such registration can be canceled by the relevant government ministry in charge if the providers disobey various ministerial corrective orders.[383] These orders can be issued to online service providers that cause "significant damage to consumers' interest" or violate a wide range of content moderation and data protection obligations.[384]

The Korean politicians sponsoring these measures argued for the need to protect users (and particularly children) and effectively paralyzed the lobbying arms of online service operators, leading to a number of unprecedented laws being adopted. These include mandatory identification laws that obligate online services to collect identity verification information from users, forcing the providers to amass huge amounts of personal data and make themselves the target of cyber attacks. While Korea's most infamous identification mandates were struck down as unconstitutional in 2012 (for general comments platforms) and in 2021 (for election-related comments platforms),[385] they still remain in effect for using mobile phone services, playing internet games, and leaving comments on public agencies' websites.[386]

The means of identity verification are not popular because they are limited to methods predetermined by the government, which tend to be expensive and cumbersome and which often require more personal data than needed.[387] It is no surprise that the Youth Protection Commission and other Korean agencies routinely highlight certain online material (and other material online or offline) as harmful to youth. Also, it is no surprise that online service providers serving content labeled as harmful to children are required to conduct age verification to comply with the rating rules. However, uniquely in Korea, online service providers are required to conduct age verification in ways that endanger privacy and data protections and therefore increase compliance costs for domestic providers.

In addition, Korea does not give online service providers a safe harbor for undesirable material posted by their customers. Instead, mandatory notice-and-takedown rules require online service providers to remove rights-infringing comments immediately after receiving notice from the affected party, forcing them to err on the side of deleting comments they are unsure of.[388] Although there is no statutory penalty, a 2009 Supreme Court decision affirmed the strict liability nature of the overall intermediary liability scheme.[389] In this case, the court held that Naver, a Korean online platform that debuted in 1999, was liable for failure to take down comments accusing the supposed victim of having impregnated a woman and then persuading her to get an abortion though Naver had no way of checking the defamatory substance of the comments. The Korean Communication Standards Commission, a national administrative body, issues takedown orders "as necessary for nurturing communications ethics."[390] More than 200,000 webpages or websites are taken down every year, some of which are not even accused of violating any legal prohibition.[391]

As for online gaming, until January 1, 2022, all internet games played by players under sixteen years old had to be shut down between 12:00 a.m. and 6:00 a.m.[392] Although the mandatory shutdown was abolished, all internet game providers still must implement features allowing young users or their legal guardians to control how much time they spend gaming.[393] The latter law necessitates and justifies the identity verification law for internet games mentioned earlier.

Meanwhile, all platforms capable of uploading videos and images for public viewing must be equipped with an upload filter that compares all files being uploaded against a precurated database of nonconsensually created or distributed sexual material, sexually defamatory deep fakes, and child sexual abuse material.[394] As a result, currently, any video being uploaded on major platforms in Korea suffers from a latency of around five to ten seconds depending on the video size, a duration that is likely to lengthen as the database of forbidden material grows larger.[395]

Another burden on all online service providers based in Korea is that they must pay transit fees (or equivalent internet access fees) to local internet service providers in amounts that widely surpass the costs of internet access in all other major cities in the world.[396] This is because Korea has the world's only mandatory rule based on the Sending Party Network Pays principle.[397]

Domestic online service providers have long complained about the regulatory burden they face, causing the Korean government, in turn, to repeatedly commission studies to assess the situation.[398] However, these problems persist, fueling aspirations for localizing foreign services and putting them under the same regulations.[399]

Trade-Based Rules on Data Localization

On a related note, data localization is a major consideration when it comes to digital trade in services. When people use YouTube, for instance, the data is often provided remotely from servers overseas. In addition, when local businesses purchase advertising time on YouTube, it may be local residents viewing those ads, but the ad content they are watching is provided remotely from servers overseas. In either case, such usage constitutes a trade in services from the locus of the YouTube servers to those of the advertisers.

Such trade in services, through cross-border supply via the internet, is increasing rapidly. Data localization requirements that remote servers providing such content, or the services themselves, be located within the country are justified as a way of leveling the playing field between foreign service providers and domestic ones, but these regulations bend or break trade rules that Korea and most developed countries have agreed to follow.

The most contentious obligations of WTO members are market access and national treatment under the General Agreement on Trade in Services (GATS). Members are prohibited, for example, from violating these two obligations listed in their respective schedules of specific commitments under GATS. According to the GATS classification of services, data localization requirements would affect the services falling under "value-added services" and "computer and related services."[400] A majority of WTO members have made liberalizing commitments on both of those services.

Although these commitments were made during the Uruguay Round of multilateral trade negotiations in the late 1980s and early 1990s before the internet became pervasive and popular, these liberalization commitments should be deemed still effective with respect to the internet, according to the decision in a case known by the shorthand *U.S.—Gambling*, in which a WTO panel announced intramodal technological neutrality in cross-border supply mode.[401] This conclusion also stems from the WTO Appellate Body's decision on a case called *China—Publications and Audiovisual Products*, which interpreted Beijing's liberalizing commitment on sound recording distribution services to include online as well as offline services.[402]

First, in terms of market access, Article XVI:2 of the GATS provides an exhaustive list of quantitative restrictions that can be sustained only by explicitly itemizing them in a country's Schedule of Commitments.[403] On the surface, data localization is a quantitative restriction, not a qualitative one. But just as the *U.S.—Gambling* decision deemed a nationality requirement as a "zero quota" imposed on overseas service providers, data localization can be deemed a quantitative restriction.[404] Indeed, data localization effectively bans the cross-border supply of services as a mode of service trade and forces foreign service providers to move into the commercial presence mode,[405] and it is likely to be considered a zero quota in violation of Article XVI.

Secondly, the national treatment norm governed by Article XVII of the GATS also bans both de jure discrimination and de facto discrimination based on nationality. Data localization applies equally to all online service providers, but (formally) equal treatment may be discriminatory in a de facto sense.[406] The WTO adjudication bodies have consistently held that the "aims" of a certain measure do not cure the discrimination in several cases, beginning with the Appellate Body's *EC—Bananas III* decision and later in its *Argentina—Financial Services* decision.[407] For instance, even if some measures have such purposes of privacy protection or national security, the key question is whether measures end up treating foreign service providers less favorably.

Korean critics may well argue that foreign online content providers are not like domestic content providers to begin with because their content is transmitted from remote locations. However, in the *U.S.—Gambling* decision, the government of Antigua argued that services should not be considered

"unlike" merely because they are provided through different modes of supply.[408] Notably, Antigua's argument prevailed in the decision.[409] Other cases have since solidified this trend: for instance, in its *Canada—Autos* decision, a WTO panel also found "likeness" between, on the one hand, the services provided on Canadian soil through a commercial presence and movement of natural persons and, on the other hand, the services provided remotely through cross-border supply and consumption abroad.[410] Thus, data localization can be said to be applicable to two like services, namely content provided *remotely* and content provided *domestically* through local servers. With that in mind, one rejoinder to critics is to ask whether Korea's current approaches violate the national treatment norm of international trade law to which the Korean government has committed itself.

To be sure, Article XIV lit. a) of the GATS does allow the adoption of measures considering the protection of public morals and the maintenance of public order, while Article XIV bis allows for security exceptions.[411] The right to adopt exceptional measures is subject to certain conditions in the chapeau to Article XIV of the GATS, which requires that they be "applied in a manner that does not constitute 'arbitrary' or 'unjustifiable' discrimination, or a 'disguised restriction on trade in services.'"[412] Just take the precedents set by *U.S.—Gambling* as an illustration: the prohibition of online gambling services from Antigua and Barbuda was held to violate the chapeau because it allowed domestic U.S. internet operators to provide the same services.[413] Since then, scholars have tried to figure out what satisfies the exception in the context of restrictions on the free flow of data but without much success.[414]

Trade Practices on Data Localization

Korea faces the same dilemma that many other countries do, namely, the conflict between its domestic practices and the international obligations it has agreed to. As with other trade issues, the possibility that data localization may violate WTO rules has not dissuaded various countries, including Korea, from engaging in or contemplating data localization. And because this is an area of international trade law where WTO cases are few and far between (limited mostly, for example, to *U.S—Gambling and China—Publications and Audiovisual Products*), rules on data localization tend to be hashed out during trade talks, not in arbitration rulings.

In 2013, U.S. trade negotiators began including "data localization" on a list of digital protectionist measures that Washington intended to oppose, alongside censorship, filtering, privacy regulations, and sometimes even lax intellectual property enforcement.[415] Starting in 2015, the EU, too, criticized Russia's and China's data localization requirements as disproportionate to "national security" concerns and, therefore, as examples of out-and-out digital protectionism.[416]

After much deliberation, the EU announced in 2018 its trade strategy toward digital protectionism taking into account these data protection concerns. Brussels proposed the following three pillars: free flow of data, a ban on data localization, and language that excludes data protection regulations from the list of barriers to trade.[417]

By 2016, the United States and the EU had been able to agree on identifying three measures as being clearly protectionist, including data localization as well as taxes on digital flows and forced technology transfers.[418] Together, Washington and Brussels have argued that these measures can lead to unanticipated side effects, including reduced internet stability, generativity, and access to information.[419]

The fact is, however, that trade law (as opposed to trade practice) does not provide a broad general normative context for evaluating various cases of data localization. No trade agreement discussing cross-border data flows, including the ones to which Korea is a party, mentions other supposedly protectionist measures such as censorship, filtering, or internet shutdowns as impermissible barriers to trade.[420] So these constitute an insufficient normative basis for discouraging other countries from enacting data localization *even* if they wanted to follow the leadership of the United States and the EU on the definition of data protectionism.

Most importantly, neither the EU nor the United States have a general theory as to when trade restrictions on information are protectionist, even when evaluating their *own* trade-restrictive policies and practices.[421] Some complain that it is not even clear whether and when privacy regulations can be exempted under the exceptions that GATS furnishes on public order or national security grounds.[422]

Given the lack of robust normative grounds, state parties *can* fall into a vicious cycle of digital protectionism begetting further digital protectionism, which forces countries to face the thorny question of whether a targeted data localization measure designed to address specific risks posed by overseas data breaches constitutes protectionism.[423] One recent example of this is the Clean Apps initiative during former U.S. president Donald Trump's tenure, which was an attempt to keep U.S. TikTok users' data on American soil and safe from potential surveillance by the Chinese Communist Party.[424]

Resolving this question requires examining the differences between data and other commodities, but it is not clear how those differences translate into a stable theory of what is protectionist, since the question of what constitutes a GATS violation is itself unclear.[425] Some have tried to square this circle by filtering the trade discussion through the question of rights: any restriction to data-based services would also, this argument runs, interfere with people's freedom of speech. This argument is particularly salient in the United States, as the State Department has advocated the "free flow of information" for decades.[426] However, some scholars conclude that trade talks focusing on "free flow of information vs. data protectionism" are ineffective and sometimes hypocritical.[427]

What Korean Critics Miss

In the end, despite the limits and difficulty of applying digital trade rules and practices, Korean policymakers have not stopped arguing for data localization rules aimed at subsidizing domestic companies that are suffering from "reverse discrimination" due to Korea's unprecedented and interventionist internet regulations.

Although trade rules allow countries like Korea to engage in various internet regulations for the purpose of protecting people's health, property, and lives, their ability to compensate in a sense for the regulatory costs that domestic companies face by forcing offshore providers to change the mode of supply has never been accepted as complying with existing trade rules.

And all of Korea's domestic internet rules can be enforced on foreign services by, for instance, blocking websites that do not meet the domestic requirements.[428] Although Korean policymakers could directly address the perceived discrimination in this way, the government simply chooses not to apply those rules,[429] probably in order to satisfy the domestic populace's desire to use foreign companies' services and to avoid the difficulties associated with requiring foreign companies to keep data in-country. There is no cause for condoning the practice of blocking the noncomplying foreign websites, but artificially created claims of discrimination should not be used to justify data localization. Furthermore, such a forthcoming approach may serendipitously bring to the fore the real problems with Korea's domestic internet rules: human rights.

A Better Focus for Korea

Data localization initiatives are known to interfere with the free flow of information. They can be motivated anywhere by security, sovereignty, privacy, taxation, or competition concerns. But in Korea, the most pronounced data localization initiatives have arisen, first, from a desire to promote fair competition between domestic Korean firms and foreign companies and, second, from the need to investigate cross-border cyber crimes.

But the Budapest Convention and a new approach to fair competition would provide a better way forward. In assessing the likelihood that Korea will accede to the Budapest Convention to assuage the need for cross-border investigations, it seems clear that the country's domestic investigatory regime could easily be updated and harmonized as required for accession to the convention. Of course, the public's concerns about privacy may generate some friction if Korea were to do so. But in the final analysis, given the Korean public's desire to migrate to foreign communication platforms whenever the privacy-infringing nature of domestic surveillance has been highlighted in the media, data localization of foreign services will likely be resisted more strongly by the Korean public than accession to the convention.

Meanwhile, even as Korea's decision on the Budapest Convention remains in limbo, Korean politicians desire for data localization is growing in another respect. They argue that foreign companies can compete and beat domestic companies because only the latter are subject to Korea's intricate internet regulations.

WTO trade rules allow exceptions for public interest purposes and therefore may be neutral to data localization initiatives. However, the WTO rules do *not* seem to allow data localization initiatives, including ones in Korea, that are motivated not by the public interest but by a desire to *enhance* the application of local laws to foreign companies. Because local laws can always be applied to foreign services

(as in the case of blocking the noncomplying websites), the public interest can be preserved, so the requirement that foreign firms establish and maintain a local presence is an unnecessary restriction on the cross-border provision of services.

Unfortunately, as long as perceptions of regulatory "reverse-discrimination" against domestic Korean companies remain, the calls in Korea for data localization will not subside. Ultimately, there is no readily available, instrument-based argument against Korea's widespread and deepening aspiration for data localization. Neither WTO trade rules nor the Budapest Convention will answer either local law enforcement's needs or local internet companies' calls for fair competition over the long term.

To push back on the fair competition argument, a solution cannot simply rely on legal principles but would need to dismantle Korea's parochial internet regulations, which provide a never-ending stream of arguments used by supporters of data localization in the name of fair competition. To do so, skeptics of data localization need to leverage concerns about human rights.

In addition, the resistance in Seoul to the Budapest Convention will weaken if Koreans realize that domestic surveillance is not any more intrusive than what is allowed in most other democracies. At that point, the convention would provide a more sustainable, instrument-based counterweight to calls in Korea for data localization. Enhanced cross-border data access under the convention would not necessarily abolish a safe haven for secret communications, while data localization would definitely do so. In this case, too, arguments and practices based on human rights could play an important role in shifting public attitudes and exerting pressure on the country's political and regulatory class.

Many data localization rules are motivated by a desire for sovereign control. They originate from an idea that data is safer, more secure, or more useful, either from a control-hungry sovereign's perspective or from that of privacy-hungry subjects, when it is located in a certain jurisdiction rather than another. However, data reflects a sentient being's perceptions of the world. The transferring of data is arguably akin to speech, and data collection is a form of knowledge. Most norms on free expression distinguish speech from physical activities and also distinguish data from physical objects. Cross-border transfers or collection of data is essentially cross-border speech or knowledge. These principles on free speech (and access to knowledge) should create exceptions to the sovereign's Westphalian control within its territory and provide ample reasons for why data localization is not a sustainable governance tool and why human rights should figure prominently in the discourse on data localization.

Even data localization for economic purposes at least in the case of Korea originates from parochial internet regulations that put domestic companies at a disadvantage vis-à-vis foreign firms, and many of these regulations depart from international standards of human rights. Instead of restricting remote modes of supply and thereby causing friction with international economic law and treaties, Korea would be better off finding a much more efficient way to balance these competing interests while upholding its commitments to international norms and human rights standards.

The author's views represent his own independent analysis and should not be understood as representing the official policy of any government.

About the Authors

EVAN A. FEIGENBAUM is a vice president for studies at the Carnegie Endowment for International Peace, where he oversees research in Washington, Beijing, and New Delhi on a dynamic region encompassing both East Asia and South Asia. He was also the 2019–2020 James R. Schlesinger Distinguished Professor at the Miller Center of Public Affairs at the University of Virginia, where he is now a practitioner senior fellow.

Initially an academic with a PhD in Chinese politics from Stanford University, Feigenbaum's career has spanned government service, think tanks, the private sector, and three major regions of Asia. From 2001 to 2009, he served at the U.S. State Department as deputy assistant secretary of state for South Asia (2007–2009), deputy assistant secretary of state for Central Asia (2006–2007), member of the policy planning staff with principal responsibility for East Asia and the Pacific (2001–2006), and an adviser on China to deputy secretary of state Robert B. Zoellick, with whom he worked closely in the development of the U.S.-China senior dialogue. Following government service, Feigenbaum worked in the private and nonprofit sectors. He was vice chairman of the Paulson Institute at the University of Chicago and the co-founder of MacroPolo, its digital venture on the Chinese economy; head of the Asia practice at the markets consultancy Eurasia Group; and senior fellow for Asia at the Council on Foreign Relations.

Before government service, he worked at Harvard University as lecturer on government in the faculty of arts and sciences and as executive director of the Asia-Pacific Security Initiative and program chair of the Chinese Security Studies Program in the John F. Kennedy School of Government, and he was lecturer of national security affairs at the U.S. Naval Postgraduate School. He is the author of three books and monographs, including *The United States in the New Asia and China's Techno-Warriors: National Security and Strategic Competition From the Nuclear to the Information Age.*

MICHAEL R. NELSON is a senior fellow in the Carnegie Endowment's Technology and International Affairs Program, which helps decisionmakers understand and address the impacts of emerging technologies, including digital technologies, biotechnology, and artificial intelligence. Prior to joining Carnegie, he started the global public policy office for Cloudflare, a startup that has improved the performance and security of more than 10 million websites around the world. Nelson has also served as a principal technology policy strategist in Microsoft's Technology Policy Group and before that was a senior technology and telecommunications analyst with Bloomberg Government. In addition, Nelson has been teaching courses and doing research on the future of the internet, cyber policy, technology policy, innovation policy, and e-government in the Communication, Culture, and Technology Program at Georgetown University.

Before joining the Georgetown faculty, Nelson was director of internet technology and strategy at IBM, where he managed a team helping define and implement IBM's next-generation internet strategy. He has served as chairman of the Information, Communication, and Computing Section of the American Association for the Advancement of Science, serves as a trustee of the Institute for International Communications, and was selected to be a "Global Leader of Tomorrow" by the World Economic Forum. From 1988 to 1993, he served as a professional staff member for the Senate's Subcommittee on Science, Technology, and Space and was the lead Senate staffer for the High-Performance Computing Act. In 1993, he joined then vice president Al Gore at the White House and worked with then president Bill Clinton's science adviser on issues relating to the Global Information Infrastructure, including telecommunications policy, information technology, encryption, electronic commerce, and information policy.

RAHUL MATTHAN is a partner with Trilegal and heads its technology, media, and telecommunications practice. He serves on the board of the firm. He is also a fellow with the Takshashila Institution's Technology and Policy Research Program. He has advised on some of the largest technology and telecom acquisitions in the country. He advises domestic and international corporations on a wide range of regulatory issues including in relation to privacy, map regulation, fintech, encryption, spectrum regulation, e-commerce, the sharing economy, biotech, digital content, and streaming media. Matthan has been involved in a number of policy initiatives including assisting the Indian government in preparing the country's privacy law as well as its unique ID law. He was a member of the Reserve Bank of India's Committee on Household Finance and was part of the committee of experts on nonpersonal data regulation. He is a frequent speaker and has a weekly column on issues at the intersection of law and technology.

TAEWOO NAM is a professor in the Department of Public Administration and Graduate School of Governance at Sungkyunkwan University in Korea. He is also a research fellow at the Center for Technology in Government at the University at Albany, State University of New York. He serves as an editorial board member for *Government Information Quarterly*, the *Policy Studies Journal*, and the *Journal of Global Information Management.* His research interests include government innovation, open

government, citizen participation, and digital government. Recent publications have appeared in leading journals related to those research interests, including *Government Information Quarterly*, *Technology in Society*, *Telematics and Informatics*, *Technological Forecasting and Social Change*, *Futures*, the *International Journal of Information Management*, *Computers in Human Behavior*, the *Social Science Computer Review*, the *Journal of Urban Technology*, the *Journal of Information Technology and Politics*, and *Information Polity.*

KYUNG SIN "KS" PARK is a professor of law at Korea University. He served as a commissioner at the Korea Communication Standards Commission, a presidentially appointed internet content regulation body (2011–2014), and as a member of the National Media Commission, an advisory body to the National Assembly set up to examine the bills allowing media crossownership and other media and internet regulations. He is the executive director of Open Net Korea and was previously the executive director of the PSPD Law Center—part of People's Solidarity for Participatory Democracy, a Seoul-based nongovernmental organization that promotes popular participation in government decisionmaking. These organizations have pursued and have won several high-profile legal cases and have pushed for legislative action in the areas of freedom of speech, privacy, net neutrality, web accessibility, digital innovation, and intellectual property.

SMRITI PARSHEERA is a fellow with the CyberBRICS Project at Fundação Getúlio Vargas (FGV) Law School in Brazil. From 2016 to 2020, she was involved in setting up and led the technology policy work at New Delhi's National Institute of Public Finance and Policy. She has also worked with the Competition Commission of India and the United Nations Development Programme and was a part of the research secretariat for India's Financial Sector Legislative Reforms Commission. Her current research interests include data governance, digital rights, competition policy, and the study of policymaking processes. She studied law at the National Law School of India University, Bangalore, and the University of Pennsylvania School of Law and is currently pursuing a PhD in the School of Public Policy at the Indian Institute of Technology Delhi.

SHREYA RAMANN is a consultant at Trilegal and is part of the technology, media, and telecommunications practice group. She has worked on legal structuring and advisory services for various clients in e-commerce, telecoms, payment and settlement systems, healthcare, and cybersecurity. She has also been involved in advising the government on policy reforms such as the nonpersonal data framework and geospatial data guidelines, as well as assisting clients with responses to significant government consultation papers on the e-commerce policy and the personal data protection framework.

Notes

Introduction

1 See, for example, Adrian Shahbaz, "Freedom on the Net 2018: The Rise of Digital Authoritarianism," Freedom House, https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

2 Nohyoung Park, "A Korean Approach to Data Localization," in *The Korean Way With Data: How the World's Most Wired Country Is Forging a Third Way*, ed. Evan A. Feigenbaum and Michael R. Nelson, Carnegie Endowment for International Peace, August 17, 2021, https://carnegieendowment.org/2021/08/17/korean-approach-to-data-localization-pub-85165; Kyung Sin "KS" Park, "Korea's Path to Best Practices for Cross-Border Data Flows," in *Data Governance, Asian Alternatives: How India and Korea Are Shaping Rules and Standards*, ed. Evan A Feigenbaum and Michael R. Nelson, Carnegi Endowment for International Peace, August 31, 2022; and Taewoo Nam, "Open Data Policy in Korea," in *Data Governance, Asian Alternatives: How India and Korea Are Shaping Rules and Standards*, ed. Evan A Feigenbaum and Michael R. Nelson, Carnegi Endowment for International Peace, August 31, 2022.

3 Smriti Parsheera, "India's Domestic Priorities and International Positioning on Cross-Border Data Flows," in *Data Governance, Asian Alternatives: How India and Korea Are Shaping Rules and Standards*, ed. Evan A. Feigenbaum and Michael R. Nelson, Carnegie Endowment for International Peace, August 31, 2022; and Indian Ministry of Electronics and Information Technology, "India's Trillion-Dollar Digital Opportunity," Indian Ministry of Electronics and Information Technology, 2019, 9, https://web.archive.org/web/20220604181319/https://www.meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf.

4 Susan Fourtané, "e-Estonia: The World's Most Advanced Digital Society," Interesting Engineering, February 24, 2020, https://interestingengineering.com/e-estonia-the-worlds-most-advanced-digital-society.

5 Diane Frank, "UK Finds New e-Gov Boss," Federal Computer Week (FCW), May 27, 2004, https://fcw.com/workforce/2004/05/uk-finds-new-e-gov-boss/235596/; and Akos Erzse and Melanie Garson, "A Leader's Guide to Building a Tech-Forward Foreign Policy," Tony Blair Institute for Global Change, March 25, 2022, https://institute.global/sites/default/files/articles/A-Leaders-Guide-to-Building-a-Tech-Forward-Foreign-Policy.pdf.

6 William J. Broad, "Clinton to Promote High Technology, With Gore in Charge," *New York Times*, November 10, 1992, https://www.nytimes.com/1992/11/10/science/clinton-to-promote-high-technology-with-gore-in-charge.html; and "Al Gore and Information Technology," Wikipedia, https://en.wikipedia.org/wiki/Al_Gore_and_information_technology.

7 Ronald H. Brown, "The Global Information Infrastructure: Agenda For Cooperation," National Telecommunications and Information Administration, June 1, 1995, https://www.ntia.doc.gov/report/1995/global-information-infrastructure-agenda-cooperation; and "The National Information Infrastructure: Agenda for Action," U.S. Department of Commerce, September 15, 1993, https://eric.ed.gov/?id=ED364215.

8 Elahe Izadi, "The White House's First Web Site Launched 20 Years Ago This Week. And It Was Amazing," *Washington Post*, October 21, 2014, https://www.washingtonpost.com/news/the-fix/wp/2014/10/21/the-white-houses-first-website-launched-20-years-ago-this-week-and-it-was-amazing.

9 Thomas H. Davenport, "Who Can Succeed Barack Obama as Digitizer in Chief?," *Fortune*, April 1, 2016, https://fortune.com/2016/04/01/who-can-succeed-barack-obama-as-digitizer-in-chief; and David K. Li, "Obama Is the Geek-in-Chief," *New York Post*, April 25, 2016, https://nypost.com/2016/04/25/obama-is-the-geek-in-chief.

10 "The World's Most Valuable Resource Is No Longer Oil, But Data," *Economist*, May 6, 2017, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

11 Antonio García Martínez, "No, Data Is NOT the New Oil," *Wired*, February 26, 2019, https://www.wired.com/story/no-data-is-not-the-new-oil; and Michael R. Nelson, "Internet Myth-Busting," *Intermedia* 47, no. 1 (April 2019), https://www.iicom.org/intermedia/intermedia-apr-2019/internet-myth-busting.

12 Harishankar Singh, "Data Is the New Fuel, AI Is the Accelerator," IBM Digital Transformation Blog, May 14, 2021, https://www.ibm.com/blogs/digital-transformation/in-en/blog/data-is-the-new-fuel-ai-is-the-accelerator.

13 Jane Barratt, "Data as Currency: What Value Are You Getting?" University of Pennsylvania Wharton School of Business, *Knowledge at Wharton*, August 27, 2019, https://knowledge.wharton.upenn.edu/article/barrett-data-as-currency.

14 Howard Ting, "Data Is Like Air—So, How Do You Contain It?," Forbes, May 11, 2022, https://www.forbes.com/sites/forbestechcouncil/2022/05/11/data-is-like-air-so-how-do-you-contain-it.

15 Dan Vesset, "Data Is the New Water," Medium, July 27, 2020, https://medium.com/digital-bulletin/data-is-the-new-water-62ed9bb5158a. (This post is based on a study on data by IDC and Qlik.)

16 "Centralized Versus Federated: State Approaches to P-20W Data Systems," National Center for Education Statistics Institute of Education Sciences, October 2012, https://nces.ed.gov/programs/slds/pdf/federated_centralized_print.pdf.

17 Ryan D. Junck, Bradley A. Klein, Akira Kumaki, Ken D. Kumayama, and Steve Kwok et al., "China's New Data Security and Personal Information Protection Laws: What They Mean for Multinational Companies," Skadden, Arps, Slate, Meagher & Flom, November 3, 2021, https://www.skadden.com/Insights/Publications/2021/11/Chinas-New-Data-Security-and-Personal-Information-Protection-Laws; Matt Burgess, "Ignore China's New Data Privacy Law at Your Peril," *Wired*, November 5, 2021, https://www.wired.com/story/china-personal-data-law-pipl; "Why China's New Data Security Law Is a Warning for the Future of Data Governance," *Foreign Policy*, January 28, 2022, https://foreignpolicy.com/2022/01/28/china-data-governance-security-law-privacy; Yvonne Lau, "Here's What Beijing's Sweeping New Data Rules Will Mean for Companies," *Fortune*, September 1, 2021, https://fortune.com/2021/09/01/china-data-security-law-beijing-management-regulation-internet; and "China's New National Privacy Law: The PIPL," Cooley, November 30, 2021, https://www.cooley.com/news/insight/2021/2021-11-30-china-new-national-privacy-law.

18 U.S. Department of Justice, "CLOUD Act Resources," U.S. Department of Justice, https://www.justice.gov/dag/cloudact.

19 Anirudh Burman and Upasana Sharma, "How Would Data Localization Benefit India," Carnegie India, April 14, 2021, https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-84291.

20 Nigel Cory and Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them," Information Technology and Innovation Foundation, July 19, 2021, https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/; and "Restrictions on International Data Flows Have Doubled in Four Years, With Measurable Economic Consequences, ITIF Reports," Information Technology and Innovation Foundation, July 19, 2021, https://itif.org/publications/2021/07/19/restrictions-international-data-flows-have-doubled-four-years-measurable.

21 Alex Pentland, Alexander Lipton, and Thomas Hardjono, *Building the New Economy: Data as Capital* (Cambridge, MA: Massachusetts Institute of Technology, 2021), https://mitpress.mit.edu/books/building-new-economy.

22 A couple of examples are the annual Internet Governance Forum conferences held under the auspices of the United Nations and the digital policy work done by the Organisation for Economic Co-operation and Development. See Internet Governance Forum (IGF), "IGF Annual Meetings Proceedings," IGF, https://www.intgovforum.org/en/content/igf-annual-meetings-proceedings; and "Internet Policy and Governance," Organisation for Economic Co-operation and Development, December 9, 2021, https://www.oecd.org/sti/ieconomy/internet-policy-and-governance.htm.

23 Adam Segal and Gordon M. Goldstein, *Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet*, (New York: Council of Foreign Relations, July 2022), https://www.cfr.org/report/confronting-reality-in-cyberspace/download/pdf/2022-07/CFR_TFR80_Cyberspace_Full_SinglePages_06212022_Final.pdf.

24 Datasphere Initiative, "About Us," Datasphere Initiative, https://www.thedatasphere.org/about-us. This initiative was started by the Internet and Jurisdiction Policy Network.

25 United Nations, "Secretary-General's Roadmap for Digital Cooperation," United Nations, May 29, 2020, https://www.un.org/en/content/digital-cooperation-roadmap/.

26 Anne-Marie Trevelyan and the UK Department for International Trade, "G7 Trade Ministers' Digital Trade Principles," Anne-Marie Trevelyan and the UK Department for International Trade, October 22, 2021, https://www.gov.uk/government/news/g7-trade-ministers-digital-trade-principles

27 Rajat Kathuria, Mansi Kedia, Gangesh Varma, and Kaushambi Bagchi, "Economic Implications of Cross Border Data Flows," Indian Council for Research on International Economic Relations and Internet and Mobile Association of India, November 2019, https://icrier.org/pdf/Economic_Implications_of_Cross-Border_Data_Flows.pdf.

28 "'India Won't Compromise Its Digital Sovereignty,': Ravi Shankar Prasad," *Hindustan Times*, June 6, 2021, https://www.hindustantimes.com/india-news/india-won-t-compromise-its-digital-sovereignty-ravi-shankar-prasad-101622919207459.html.
29 "What Is the Cross-Border Privacy Rules System," Asia-Pacific Economic Cooperation, October 2021, https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system.

Chapter 1

30 Arvind Gupta and Philip E. Auerswald, "The Ups and Downs of India's Digital Transformation," *Harvard Business Review*, May 2019, https://hbr.org/2019/05/the-ups-and-downs-of-indias-digital-transformation.
31 Telecom Regulatory Authority of India, "Consultation Paper on Regulatory Framework for Promoting Data Economy Through Establishment of Data Centres, Content Delivery Networks, and Interconnect Exchanges in India," Telecom Regulatory Authority of India, Consultation Paper No.10/2021, https://www.trai.gov.in/sites/default/files/CP_16122021_0.pdf. The report states that—based on "the cost of manpower, real estate, and bandwidth"—data storage in India is "at least 60 percent cheaper" than in the United States or Singapore.
32 In 1985, the IT industry exported software and services worth $25 million. See Devesh Kapur, "Causes and Consequences of India's IT Boom," *University of Pennsylvania India Review* 1, no. 2 (April 2022), https://casi.sas.upenn.edu/sites/default/files/bio/uploads/Causes_and_Consequences_of_IT_Boom.pdf.
33 Ibid.
34 United States International Trade Administration, "India - Country Commercial Guide," United States International Trade Administration, October 22, 2021, https://web.archive.org/web/20220727072457/https://www.trade.gov/country-commercial-guides/india-information-and-communication-technology.
35 Kapur, "Causes and Consequences of India's IT Boom."
36 Ibid.
37 Deloitte, "Technology, Media, and Telecommunications - Predictions 2022," Deloitte, February 2022, https://www2.deloitte.com/in/en/pages/technology-media-and-telecommunications/articles/tmt-predictions-2022.html; and World Bank, "Population, Total - India," World Bank, 2021, https://data.worldbank.org/indicator/SP.POP.TOTL?locations=IN.
38 National Payments Corporation of India, "UPI Product Statistics," National Payments Corporation of India, https://www.npci.org.in/what-we-do/upi/product-statistics.
39 This can be seen in the use of the Data Empowerment and Protection Architecture in the Reserve Bank of India's Account Aggregator Framework. See Reserve Bank of India, "Master Direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Direction, 2016," Reserve Bank of India, October 5, 2021, https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598.
40 NITI Aayog, "National Health Stack: Strategy and Approach," NITI Aayog, July 2018, https://web.archive.org/web/20220215102833/https://abdm.gov.in/publications/NHS_Strategy_and_Approach; and NITI Aayog, "Data Empowerment and Protection Architecture," August 2020, https://www.niti.gov.in/sites/default/files/2020-09/DEPA-Book.pdf.
41 Indian Ministry of Commerce and Industry, "ONDC Project," Indian Ministry of Commerce and Industry, April 2022, https://pib.gov.in/Pressreleaseshare.aspx?PRID=1814143.
42 Kapur, "Causes and Consequences of India's IT Boom."
43 Ibid.
44 India Code, "Information Technology Act, 2000," India Code, https://web.archive.org/web/20220303025038/https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf.
45 Digital India, "About Digital India," Digital India, https://www.digitalindia.gov.in.
46 Digital India, "Bharat Broadband Network (BBN)," Digital India, https://digitalindia.gov.in/content/bharat-broadband-network-bbnl; Digital India, "Universal Access to Mobile Connectivity," Digital India, https://digitalindia.gov.in/content/universal-access-mobile-connectivity; and Indian Ministry of Housing and Urban Affairs, "Smart Cities: Vision," Indian Ministry of Housing and Urban Affairs, https://smartcities.gov.in/#:~:text=Vision,that%20leads%20to%20Smart%20outcomes.
47 Indian Ministry of Electronics and Information Technology, "India's Trillion-Dollar Digital Opportunity," Indian Ministry of Electronics and Information Technology, https://www.meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf; and Indian Ministry of Commerce and Industry, "Vision of a USD 5 Trillion Indian Economy," Indian Ministry of Commerce and Industry, October 11, 2018, https://pib.gov.in/Pressreleaseshare.aspx?PRID=1549454.

48 Tanuj Bhojwani, "The Best Way Forward for Privacy Is to Open Up Your Data," iSPIRT, August 21, 2017, https://pn.ispirt.in/the-best-way-forward-for-privacy-is-to-open-up-user-data; and India Stack, "India Stack," India Stack, https://indiastack.org.

49 Nandan Nilekani, "India's Aadhaar System: Bringing E-Government to Life," Chandler Institute of Governance, *Governance Matters Magazine*, 2021, https://www.chandlerinstitute.org/governancematters/indias-aadhaar-system-bringing-e-government-to-life.

50 Ibid.

51 Unique Identification Authority of India, "Aadhaar Dashboard," Unique Identification Authority of India, https://uidai.gov.in/aadhaar_dashboard; and World Bank, "Population, Total – India."

52 Deepa Krishnan, "What the World Can Learn From the India Stack," *Strategy and Business*, December 6, 2021, https://www.strategy-business.com/article/What-the-world-can-learn-from-the-India-Stack; and National Portal of India, "Pradhan Mantri Garib Kalyan Yojana / Package," National Portal of India, September 7, 2020, https://www.india.gov.in/spotlight/pradhan-mantri-garib-kalyan-package-pmgkp.

53 Direct Benefit Transfer (DBT) Bharat, "Estimated Benefits/Gains From DBT and Other Governance Reforms," DBT Bharat, https://www.dbtbharat.gov.in/estimatedgain.

54 Unique Identification Authority of India, "Aadhaar Dashboard."

55 World Bank, "Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19," World Bank, 2021, https://www.worldbank.org/en/publication/globalfindex.

56 World Bank, "Private Sector Economic Impacts From Identification Systems," World Bank, 2018, https://documents1.worldbank.org/curated/en/219201522848336907/pdf/Private-Sector-Economic-Impacts-from-Identification-Systems.pdf.

57 "Reliance Jio 4G Claims It Crossed 16 Million Subscribers in First Month," *Indian Express*, October 10, 2016, https://indianexpress.com/article/technology/tech-news-technology/reliance-jio-creates-world-record-16-million-subscribers-in-one-month-3073468; and "Reliance Jio Crosses 50 Million Subscriber Mark in 83 Days," *Indian Express*, https://indianexpress.com/article/technology/tech-news-technology/reliance-jio-crosses-50-million-subscriber-mark-in-83-days-4400972.

58 National Payments Corporation of India, "Product Overview: Unified Payments Interface," National Payments Corporation of India, https://www.npci.org.in/what-we-do/upi/product-overview.

59 National Payments Corporation of India, "UPI Product Statistics."

60 See PhonePe, "PhonePe," PhonePe, https://www.phonepe.com; Google, "Google Payments," Google, https://pay.google.com/payments/u/0/home; WhatsApp, "WhatsApp Payments," WhatsApp, https://www.whatsapp.com/payments/in; and Amazon, "Unified Payment Interface (UPI) - FAQs," Amazon, https://www.amazon.in/gp/help/customer/display.html?nodeId=202212990.

61 See this letter from Google to the U.S. Federal Reserve. Mark Isakowitz, "Re: Federal Reserve Actions to Support Interbank Settlement of Faster Payments, Docket No. OP 1670," Google, November 7, 2019, https://www.federalreserve.gov/SECRS/2019/December/20191227/OP-1670/OP-1670_110719_136981_396266957468_1.pdf.

62 India Cellular and Electronics Association, "Contribution of Smartphones to Digital Governance in India," India Cellular and Electronics Association, July 2020, https://web.archive.org/web/20220209070433/https://icea.org.in/wp-content/uploads/2020/07/Contribution-of-Smartphones-to-Digital-Governance-in-India-09072020.pdf; "India to Have 820 Million Smartphone Users by 2022," *Economic Times*, July 9, 2020, https://economictimes.indiatimes.com/industry/telecom/telecom-news/indian-to-have-820-million-smartphone-users-by-2022/articleshow/76876369.cms?from=mdr.

63 Kantar, "Internet Adoption in India: ICUBE 2020," Kantar, June 2021, https://images.assettype.com/afaqs/2021-06/b9a3220f-ae2f-43db-a0b4-36a372b243c4/KANTAR_ICUBE_2020_Report_C1.pdf.

64 Indian Ministry of Finance, "Economic Survey 2021–22," Indian Ministry of Finance, 302, https://www.indiabudget.gov.in/economicsurvey.

65 Ericsson, "Mobile Data Traffic Outlook," Ericsson, https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/mobile-traffic-forecast.

66 European Commission, "European Commission Data Strategy: Next-Generation Digital Commission," European Commission, https://ec.europa.eu/info/sites/default/files/strategy/decision-making_process/documents/c_2022_4388_1_en_act.pdf.

67 European Commission, "A European Approach to Artificial Intelligence," European Commission, June 30, 2022, https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence.

68 Soumyarendra Barik, "Explained: Why the Govt Has Withdrawn the Personal Data Protection Bill, and What Happens Now," *Indian Express*, August 6, 2022, https://indianexpress.com/article/explained/explained-sci-tech/personal-data-protection-bill-withdrawal-reason-impact-explained-8070495/lite.

69 Indian Ministry of Communications and Information Technology, "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011," Indian Ministry of Communications and Information Technology, April 11, 2011, https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf.
70 Indian Ministry of Electronics and Information Technology, "White Paper of the Committee of Experts on a Data Protection Framework for India," Indian Ministry of Electronics and Information Technology, https://web.archive.org/web/20220331220953/https:/www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf.
71 Sreenidhi Srinivasan and Namrata Mukherjee, "Building an Effective Data Protection Regime," Vidhi Centre for Legal Policy, 2017, https://www.scribd.com/document/338204284/Building-an-effective-data-protection-regime-in-India.
72 Supreme Court of India, "Justice K.S. Puttaswamy (Retd.) and Another Petitioner(s) Versus Union of India and Others Respondent(s)," Supreme Court of India, Judgement, September 26, 2018, https://uidai.gov.in/images/news/Judgement_26-Sep-2018.pdf; and Supreme Court of India, "Justice K.S. Puttaswamy (Retd.) and Anr. Versus Union of India and Ors.," Supreme Court of India Writ Petition (Civil) No. 494 of 2012, August 24, 2017, https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.
73 Indian Ministry of Electronics and Information Technology, "Report by the Committee of Experts on Non-Personal Data Governance Framework," Indian Ministry of Electronics and Information Technology, December 16, 2020, mygov_160922880751553221.pdf.
74 Indian Ministry of Electronics and Information Technology, "White Paper of the Committee of Experts on a Data Protection Framework for India"; and Indian Ministry of Electronics and Information Technology, "Personal Data Protection Bill, 2018," Indian Ministry of Electronics and Information Technology, https://web.archive.org/web/20220202023216/https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.
75 Parliament of India, Lok Sabha, "Personal Data Protection Bill, 2019," Lok Sabha, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.
76 Parliament of India, Lok Sabha, "Report of the Joint Committee on Personal Data Protection Bill, 2019," Seventeenth Lok Sabha, December 2021, http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf.
77 PRS Legislative Research, "Annual Policy Review 2021–2022," PRS Legislative Research, May 2022, https://prsindia.org/files/policy/policy_annual_policy_review/Annual%20Policy%20Review/2022-05-10/APR_2021-22.pdf.
78 DP Bill Section 3(33); and Lok Sabha, "Report of the Joint Committee on Personal Data Protection Bill, 2019."
79 European Parliament and Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)," European Parliament and Council of the European Union, April 27, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN. See Article 4.
80 DP Bill Section 3(41); and Pawan Bali, "Data Protection Draft Bill Holds Hope for Privacy," *Asian Age*, July 28, 2018, https://www.asianage.com/india/all-india/280718/data-protection-draft-bill-holds-hope-for-privacy.html.
81 See DP Bill Section 3(15).
82 Ibid., Section 3(16); and Supreme Court of India, "Justice K.S. Puttaswamy (Retd.) and Another Petitioner(s) Versus Union of India and Others Respondent(s)."
83 See DP Bill Section 11.
84 Ibid., Chapter III.
85 Ibid., Chapter V.
86 Ibid., Section 3(11).
87 Ibid., Sections 21(1) and 23(3).
88 Ibid., Section 26.
89 Amber Sinha and Elonnai Hickok, "The Srikrishna Committee Data Protection Bill and Artificial Intelligence in India," Centre for Internet and Society, September 3, 2018, https://cis-india.org/internet-governance/blog?b_start%3Aint=930.
90 Arya Tripathy and Rishi Sehgal, "India's New Data Protection Bill, 2021: Overview and Analysis of JPC Draft," PSA Legal Counsellors, December 20, 2021, https://www.psalegal.com/indias-new-data-protection-bill-2021-overview-and-analysis-of-jpc-draft.
91 DP Bill Sections 27 and 28.
92 Ibid., Section 30.

93 European Commission, "Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)," European Commission, November 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767; and Council of the EU, "Council Approves Data Governance Act," Council of the EU, May 16, 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/05/16/le-conseil-approuve-l-acte-sur-la-gouvernance-des-donnees.

94 DB Bill Section 3(8).

95 For example, under GDPR, data principals below the age of sixteen years are considered children, and member states may provide for a lower age up to thirteen years. See European Parliament and Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)."

96 DB Bill Sections 16(2) and 16(3); and Vikram Jeet Singh, "An Introduction to India's New Privacy Regime," International Bar Association, June 22, 2022, https://www.ibanet.org/an-introduction-to-India-new-privacy-regime.

97 DP Bill Section 34; and Deloitte, "Draft Personal Data Protection Bill, 2019," Deloitte, January 2020, https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-draft-personal-data-protection-bill-noexp.pdf.

98 DP Bill Section 33(3).

99 Ibid., Section 65.

100 Section 3(23) of the DP Bill defines harm to include "(i) bodily or mental injury; (ii) loss, distortion or theft of identity; (iii) financial loss or loss of property; (iv) loss of reputation or humiliation; (v) loss of employment; (vi) any discriminatory treatment; (vii) any subjection to blackmail or extortion; (viii) any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal; (ix) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled; (x) any observation or surveillance that is not reasonably expected by the data principal;" (xi) psychological manipulation which impairs the anatomy of the individual; or (xii) such other harm as may be prescribed. See DP Bill Section 3(23); and Vijayashankar Na, "PDPA 2021: Regulating the Human Perceptions," Naavi.org, August 16, 2022, https://www.naavi.org/wp/pdpa-2021-regulating-the-human-perceptions.

101 UK Parliament, "Online Safety Bill (As Amended in Public Bill Committee)," UK Parliament, Bill 121, https://publications.parliament.uk/pa/bills/cbill/58-03/0121/220121.pdf. For more information, see Edina Harbinja, "The UK's Online Safety Bill: Not That Safe, After All?," *Lawfare* (blog), July 8, 2021, https://www.lawfareblog.com/uks-online-safety-bill-not-safe-after-all.

102 Dia Rekhi, "Global IT Bodies Express Concern Over Data Protection Bill," *Economic Times, March 2, 2022,* https://economictimes.indiatimes.com/tech/information-tech/global-it-bodies-express-concern-over-data-protection-bill/articleshow/89930675.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst; and Surajeet Das Gupta, "India's Data Localisation Rules to Be a Barrier to Digital Trade: US," *Business Standard*, April 11, 2022, https://www.business-standard.com/article/economy-policy/india-s-data-localisation-rules-to-be-a-barrier-to-digital-trade-us-122041100008_1.html.

103 Gupta, "India's Data Localisation Rules to Be a Barrier to Digital Trade: US."

104 Rekhi, "Global IT Bodies Express Concern Over Data Protection Bill."

105 Unless otherwise noted, the insights from this part of the analysis come from the committee's report. See Indian Ministry of Electronics and Information Technology, "Report by the Committee of Experts on Non-Personal Data Governance Framework."

106 Dvara Research, "Comments to the Joint Parliamentary Committee (JPC) on the Personal Data Protection Bill 2019 Introduced in the Lok Sabha on 11 December 2019," Dvara Research, https://www.dvara.com/research/wp-content/uploads/2020/03/Dvara-Research-Final-Submission-Comments-to-the-Joint-Parliamentary-Committee-on-PDP-Bill.pdf.

107 DP Bill Section 92(2) and 94(2)(e); and Prahalad Sriram, "Reconciling Localization Mandate of the Personal Data Protection Bill, 2019 With International Trade Obligations," *Narsee Monjee Institute of Management Studies (NMIMS) Law Review* 2 (June 2020): 273–284, http://lawreview.nmims.edu/wp-content/uploads/2020/07/Volume-II-NMIMS-Law-Review.pdf.

108 Indian Ministry of Electronics and Information Technology, "Report by the Committee of Experts on Non-Personal Data Governance Framework"; and Astha Kapoor, Sarada Mahesh, and Vinay Narayan, "Impact of the Non-Personal Data Governance Framework on the Indian Agricultural Sector," Aapti Institute, February 2022, https://thedataeconomylab.com/wp-content/uploads/2022/02/Aapti-Report-Impact-of-the-Non-Personal-Data-Governance-Framework-on-the-Indian-Agricultural-Sector_Final.pdf.

109 U.S Department of Health and Human Services, "Demand-Driven Open Data," U.S Department of Health and Human Services, https://web.archive.org/web/20220120211847/https://www.hhs.gov/cto/projects/demand-driven-open-data/index.html.

110 Cuts International, "Cuts Comments on the Revised Report of the Committee of Experts on Non-Personal Data Governance Framework," Cuts International, January 31, 2021, https://cuts-ccier.org/pdf/comments-on-revised_npd-governance-framework.pdf.

111 Centre for Information Policy Leadership and DSCI, "Enabling Accountable Data Transfers from India to the United States Under India's Proposed Personal Data Protection Bill (No. 373 of 2019)," Centre for Information Policy Leadership and DSCI, August 2020, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-dsci_report_on_enabling_accountable_data_transfers_from_india_to_the_united_states_under_indias_proposed_pdpb__8_september_2020_.pdf.

112 "Why Non-Personal Data Governance Framework Needs a Rethink," *Financial Express*, August 31, 2020, https://www.financialexpress.com/opinion/why-non-personal-data-governance-framework-needs-a-rethink/2069892.

113 Indian Ministry of Science and Technology, "National Data Sharing and Access Policy," Indian Ministry of Science and Technology, 2012, 10–15, https://dst.gov.in/sites/default/files/nsdi_gazette_0.pdf.

114 India Urban Data Exchange, "Unleashing the Power of Data for Public Good," India Urban Data Exchange, https://iudx.org.in; Open Budgets India, "Making India's Budgets Open, Usable, and Easy to Comprehend," Open Budgets India, https://openbudgetsindia.org; NITI Aayog, "National Data and Analytics Platform: Vision Document," NITI Aayog, January 2020, https://www.niti.gov.in/sites/default/files/2020-01/Vision_Document_30_Jan.pdf; and Sam Neufeld, "Deploying Open Government Data for AI-Enabled Public Interest Technologies," Observer Research Foundation, July 21, 2021, https://www.orfonline.org/expert-speak/ai-driven-public-interest-technologies-employing-open-government-data-achieve.

115 Indian Ministry of Electronics and Information Technology, "India Data Accessibility and Use Policy (Draft)," Indian Ministry of Electronics and Information Technology, February 2022, https://web.archive.org/web/20220314080207/https://www.meity.gov.in/writereaddata/files/Draft%20India%20Data%20Accessibility%20and%20Use%20Policy_0.pdf; and Indian Ministry of Electronics and Information Technology, "National Data Governance Framework Policy (Draft)," Indian Ministry of Electronics and Information Technology, May 2022, https://web.archive.org/web/20220719055047/https://www.meity.gov.in/writereaddata/files/National%20Data%20Governance%20Framework%20Policy_26%20May%202022.pdf.

116 For a detailed description of the DEPA framework, please see NITI Aayog, "Data Empowerment and Protection Architecture." Also see Vikas Kathuria, "Data Empowerment and Protection Architecture: Concept and Assessment," Observer Research Foundation, August 2021, https://www.orfonline.org/research/data-empowerment-and-protection-architecture-concept-and-assessment.

117 Reserve Bank of India, "Master Direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Direction, 2016."

118 National Digital Health Mission, "National Digital Health Mission: Health Data Management Policy," National Digital Health Mission, https://ndhm.gov.in/health_management_policy.

119 Sahamati, "Current List of AAs," Sahamati, https://sahamati.org.in/account-aggregators-in-india.

120 Sahamati, "Live Dashboard," Sahamati, https://sahamati.org.in/aa-dashboard.

121 Ann Cavoukian, "Privacy by Design: The 7 Foundational Principles," International Association of Privacy Professionals, January 2011, https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.

122 NITI Aayog, "National Health Stack: Strategy and Approach."

123 Open Government Data Platform India, Ministry of Electronics and Information Technology National Informatics Centre, and State Government of Sikkim, "Discover Datasets by Sector (Sikkim)," Open Government Data Platform India, Ministry of Electronics and Information Technology National Informatics Centre, and State Government of Sikkim, https://sikkim.data.gov.in; and Surat Municipal Corporation Open Data Initiative, "Open Government Data Portal of Surat City," Surat Municipal Corporation Open Data Initiative, https://www.re3data.org/repository/r3d100012679.

124 Open Government Platform, "Table of Contents," Open Government Platform, https://ogpl.github.io/index-en.html; and Dimple Patel, "Research Data Management: A Conceptual Framework," *Library Review*, July 4, 2016, https://www.emerald.com/insight/content/doi/10.1108/LR-01-2016-0001/full/html.

125 Anirudh Burman, "Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?," Carnegie India, March 9, 2020, https://carnegieindia.org/2020/03/09/will-india-s-proposed-data-protection-law-protect-privacy-and-promote-growth-pub-81217.

126 Amba Kak and Samm Sacks, "Shifting Narratives and Emergent Trends in Data-Governance Policy," Yale Law School Paul Tsai China Center, AI Now, and New America, August 2021, https://law.yale.edu/sites/default/files/area/center/china/document/shifting_narratives.pdf.

127 NITI Aayog, "Data Empowerment and Protection Architecture."

128 Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999), https://lessig.org/product/code.
129 "MediaNama: Discussion on the Governance of Non Personal Data," YouTube video, 3:55:20, posted by "MediaNama," January 15, 2021, https://www.youtube.com/watch?v=9ynaYd1_A3A.
130 Indian Ministry of Finance, "Economic Survey 2021–22."
131 Indian Ministry of Electronics and Information Technology, "Report by the Committee of Experts on Non-Personal Data Governance Framework."
132 Indian Ministry of Electronics and Information Technology, Committee of Experts Under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians* (New Delhi: Committee of Experts Under the Chairmanship of Justice B.N. Srikrishna, https://web.archive.org/web/20220809182239/https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.
133 Arindrajit Basu, "We Need a Better AI Vision," Centre for Internet and Society, October 12, 2019, https://cis-india.org/internet-governance/front-page/blog?b_start%3Aint=1050; and Indian Department for Promotion of Industry and Internal Trade, "Draft National E-Commerce Policy: India's Data for India's Development," Indian Department for Promotion of Industry and Internal Trade, February 23, 2019, https://dpiit.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf.
134 For instance, a Netflix database was deanonymized by comparing rankings and time stamps with data sets from other sources. See Arvind Narayanan and Vitaly Shmatikov, "Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset)," University of Texas at Austin, February 5, 2008, https://arxiv.org/pdf/cs/0610105.pdf. For more examples, see "Re-Identification of Anonymised Data Sets," DigiTorc, April 10, 2019, https://www.digitorc.com/re-identification-of-anonymised-data-sets.
135 Japanese Ministry of Foreign Affairs, "G-20 Osaka Leaders Declaration," Japanese Ministry of Foreign Affairs, June 29, 2019, https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html.
136 See, for example, European Parliament and Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)"; and European Commission, "European Data Strategy: Making the EU a Role Model for a Society Empowered by Bata," European Commission, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.
137 The Personal Information Protection Law restricts or bans data transfers if they harm China's national security, which is defined more broadly than in most other countries. It also requires all data processed by national agencies and critical information infrastructure operators be stored in China. Entities that handle personal information reaching a certain threshold are also required to store user data within China. See Standing Committee of the Thirteenth National People's Congress, "Personal Information Protection Law of the People's Republic of China," translated by Rogier Creemers and Graham Webster, Digichina (Stanford University), September 7, 2021, https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021.
138 Various Russian laws such as Federal Law No. 152-FZ on Personal Data contain data localization provisions and prescribe import substitutions for IT products used by government agencies, state-owned corporations, and critical infrastructure. See International Committee of the Red Cross, "Federal Law No. 152 FZ on Personal Data, 2006," International Committee of the Red Cross, July 27, 2006, https://ihl-databases.icrc.org/applic/ihl/ihl-nat.nsf/implementingLaws.xsp?documentId=874FC74312B61FFAC1257EF200543AB8&action=openDocument&xp_countrySelected=RU&xp_topicSelected=GVAL-992BUA&from=topic&SessionID=DUJCM3QC81. In Egypt's case, Law No. 151 of 2020 prohibits the transfer of personal data to recipients located outside Egypt except with the permission of the Egyptian Data Protection Center. See International Labour Organization, "Law No. 151 of 2020: Promulgating the Personal Data Protection Law," International Labour Organization, 2020, https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/111246/138543/F217894882/EGY111246%20Eng.pdf.
139 Indian Ministry of Commerce and Industry, "Shri Piyush Goyal Participates in the G-20 Meeting of the Trade and Investment Ministers," Indian Ministry of Commerce and Industry, September 22, 2020, https://pib.gov.in/PressReleseDetail.aspx?PRID=1657874.
140 United Nations (UN) Conference on Trade and Development, *Digital Economy Report 2021: Cross-border Data Flows and Development: For Whom the Data Flow* (New York: UN Conference on Trade and Development, 2021), https://unctad.org/system/files/official-document/der2021_en.pdf.
141 Nima Elmi, "Is Big Tech Setting Africa Back?," *Foreign Policy*, November 11, 2020, https://foreignpolicy.com/2020/11/11/is-big-tech-setting-africa-back.

142 Nigeria has required all subscriber and consumer data of ICT service providers as well as all government data to be stored locally within the country since December 2013 through the Guidelines for Nigerian Content Development in ICT. See Nigerian National Information Technology Development Agency (NITDA), "Guidelines for Nigerian Content Development in Information and Communication Technology (ICT)," NITDA, August 2019, https://nitda.gov.ng/wp-content/uploads/2020/11/GNCFinale2211.pdf. In Rwanda, the concept of data sovereignty has been at the core of the government's Data Revolution Policy, which requires that national data should be hosted locally. See Rwandan National Institute of Statistics, "Data Revolution," Rwandan National Institute of Statistics, https://www.statistics.gov.rw/content/data-revolution#:~:text=The%20Data%20Revolution%20Policy%20(DRP,open%20license%20and%20technical%20standards. A 2012 law states that all critical information data within the government should be hosted in one central national data center. See Rwanda Law Reform Commission, "Ministerial Order N°001/MINICT/2012 of 12/03/2012 (Ministerial Instructions Related to the Procurement of Information and Communications Technology Goods and Services by Rwanda Public Institutions," Rwanda Law Reform Commission, March 12, 2012, https://www.rlrc.gov.rw/fileadmin/user_upload/Laws/Laws/RWA%20LAWS%20PUBLISHED%20IN%202012/RWA%202012%20%20%20MI%20N0%20001-MINICT-2012%20%20PROCUREMENT%20OF%20INFO%20AND%20COMMS%20TECHNOLOGY%20GOOD%20AND%20SERVICES%20BY%20RDA%20PUBLIC%20INSTITUTIONS%20%20%20-%20OG%20N0%2011BIS%20%20OF%2012%20%20MARCH%202012.pdf.

Chapter 2

143 Statistics Korea, "Open Data Portal," Statistics Korea, https://www.data.go.kr/en/index.do; and Statistics Korea, "Information Disclosure at a Glance," Statistics Korea, https://www.open.go.kr/com/main/mainView.do.
144 Korea Data Agency, "About MyData," Korea Data Agency, https://www.kdata.or.kr/kr/contents/mydata_01/view.do.
145 Korean Ministry of Interior and Safety, "Organizational Chart," Korean Ministry of Interior and Safety, https://www.mois.go.kr/eng/sub/a02/organChart/screen.do.
146 Korean Ministry of Science and Information and Communications Technology (ICT), "Organization," Korean Ministry of Science and ICT, https://www.msit.go.kr/eng/contents/cont.do?sCode=eng&mPid=19&mId=25.
147 Statistics Korea, "History," Statistics Korea, http://kostat.go.kr/portal/eng/aboutUs/2/1/index.static.
148 Personal Information Protection Commission, "Vision and Mission," Personal Information Protection Commission, https://www.pipc.go.kr/eng/user/itc/visionMission.do.
149 The Presidential Committee on the Fourth Industrial Revolution, "About PCFIR," The Presidential Committee on the Fourth Industrial Revolution, https://www.4th-ir.go.kr/en/greetings.
150 The Presidential Committee on the Fourth Industrial Revolution, "Data 119," The Presidential Committee on the Fourth Industrial Revolution, https://web.archive.org/web/20220613225537/https://www.4th-ir.go.kr/en/data119.
151 Open Data Strategy Council, "The Public Data Strategy Committee," Open Data Strategy Council, https://www.odsc.go.kr.
152 Open Data Strategy Council, "Introduction on Open Data," Open Data Strategy Council, https://www.odsc.go.kr/eng.
153 Open Data Mediation Committee, "About Open Data Mediation Committee," Open Data Mediation Committee, https://www.odmc.or.kr/eng.
154 Korean Legislation Research Institute, "Framework Act on Intelligent Informatization," Korea Law Translation Center, https://elaw.klri.re.kr/kor_service/lawView.do?hseq=54720&lang=ENG.
155 Korean Legislation Research Institute's Korea Law Translation Center, "Personal Information Protection Act," Korean Legislation Research Institute's Korea Law Translation Center, https://elaw.klri.re.kr/kor_service/lawView.do?hseq=53044&lang=ENG.
156 Korean Legislation Research Institute's Korea Law Translation Center, "Act on Promotion of the Provision and Use of Public Data," Korean Legislation Research Institute's Korea Law Translation Center, https://elaw.klri.re.kr/kor_service/lawView.do?hseq=47133&lang=ENG.
157 Korean Legislation Research Institute's Korea Law Translation Center, "Act on the Promotion of Data-based Administration," Korean Legislation Research Institute's Korea Law Translation Center, https://elaw.klri.re.kr/kor_service/lawView.do?hseq=54647&lang=ENG.
158 Korean Legislation Research Institute's Korea Law Translation Center, "Act on the Promotion of Data-based Administration."
159 Korean Legislation Research Institute's Korea Law Translation Center, "Electronic Government Act," Korean Legislation Research Institute's Korea Law Translation Center, https://elaw.klri.re.kr/kor_service/lawView.do?hseq=56406&lang=ENG.

160 Korean Legislation Research Institute's Korea Law Translation Center, "Act on the Promotion of Smart City Development and Industry," Korean Legislation Research Institute's Korea Law Translation Center, https://elaw.klri.re.kr/kor_service/lawView.do?hseq=54507&lang=ENG.
161 Korean Legislation Research Institute's Korea Law Translation Center, "Act on Promotion of the Provision and Use of Public Data."
162 Taewoo Nam, "How Did Korea Use Technologies to Manage the COVID-19 Crisis? A Country Report," *International Review of Public Administration* 25 (2021): 225–242, https://doi.org/10.1080/12294659.2020.1848061.
163 Open Government Partnership, "About Open Government Partnership," Open Government Partnership, https://www.opengovpartnership.org/about/.
164 Byeong-jin Jeon and Hee-Woong Kim, "An Exploratory Study on the Sharing and Application of Public Open Big Data," *Informatization Policy* (2017): 27–41, https://papersearch.net/thesis/article.asp?key=3578603.
165 Presidential Committee on the Fourth Industrial Revolution, "About PCFIR."
166 Korea Data Agency, "2021 Data Industry White Book," Korea Data Agency, https://www.kdata.or.kr/kr/whitePaper/view.do.
167 Korean Legislation Research Institute's Korea Law Translation Center, "Act on the Promotion of Data-based Administration"; and Korean Legislation Research Institute's Korea Law Translation Center, "Statistics Act," Korean Legislation Research Institute's Korea Law Translation Center, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=44517&lang=ENG.
168 Korean Anti-Corruption and Civil Rights Commission, "Introduction to Inactive Administration," Korean Anti-Corruption and Civil Rights Commission, https://www.epeople.go.kr/nep/pttn/negativePttn/NegativePttnCotents.npaid.
169 Korea Data Agency, "2021 Data Industry Survey," Korea Data Agency, March 31, 2022, https://www.kdata.or.kr/kr/board/info_01/boardView.do?pageIndex=1&bbsIdx=33253&searchCondition=all&searchKeyword=.
170 Hyerim Son, "Data-based Administration, No Budget and No People," *Busan Ilbo*, June 29, 2012, http://www.busan.com/view/busan/view.php?code=2021062919264327694.
171 Wookjoon Sung, "The Big Data Policy in the Public Sector From the Data Life Cycle Perspective," *Journal of Korean Association for Regional Information Society*, 20 (2017): 25–41, https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002235943.
172 United Nations (UN) Department of Economic and Social Affairs, "UN e-Government Surveys," UN Department of Economic and Social Affairs, 2020, https://publicadministration.un.org/en/Research/UN-e-Government-Surveys; and Organisation for Economic Co-operation and Development (OECD), "OECD Digital Government Index," OECD, https://goingdigital.oecd.org/indicator/58.
173 Seung-joo Hahn, "An Exploratory Study on Professional Identity and Accountability of Civil Servants," *Korean Review of Organizational Studies*, 13 (2017): 1–32, https://www.dbpia.co.kr/Journal/articleDetail?nodeId=NODE07104052.

Chapter 3

174 Indian Ministry of Electronics and Information Technology, "India's Trillion-Dollar Digital Opportunity, Indian Ministry of Electronics and Information Technology, 2019, https://web.archive.org/web/20220604181319/https://www.meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf.
175 Ibid., 9.
176 For instance, the report by the joint parliamentary committee encourages a push for sovereignty by noting, "India may no more leave its data to be governed by any other country." See Joint Committee on the Personal Data Protection Bill, 2019 (Joint Parliamentary Committee), *Report of the Joint Committee on the Personal Data Protection Bill*, 2019 (New Delhi: Lok Sabha Secretariat, December 16, 2021), 41, http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf.
177 Hinrich Foundation, All India Management Association, and AlphaBeta, "The Digital Opportunity: The Promise of Digital Trade for India," 2019, 17, 24, https://alphabeta.com/wp-content/uploads/2019/08/digitrade_india.pdf.
178 Chaim Gartenberg, "Big Tech's 2021 Earnings Were Off the Chart," *Verge*, February 11, 2022, https://www.theverge.com/2022/2/11/22925859/big-tech-companies-2021-earnings-record-revenue-apple-amazon-alphabet-meta.
179 Urvashi Aneja and Angelina Chamuah, "A Balancing Act: The Promise and Peril of Big Tech in India," Tandem Research, 2020, https://www.responsibletech.in/post/big-tech-in-india; and Richard Blumenthal, Brian Schatz, Ron

Wyden, Elizabeth Warren, and Christopher A. Coons et. al., "Letter to FTC Chairperson Lina Khan," September 20, 2021, https://www.blumenthal.senate.gov/imo/media/doc/2021.09.20%20-%20FTC%20-%20Privacy%20Rulemaking.pdf.

180 Nigel Cory and Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them," Information Technology and Innovation Foundation, July 19, 2021, https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost.

181 Ibid.

182 Japanese Ministry of Foreign Affairs, "Osaka Declaration on Digital Economy," Japanese Ministry of Foreign Affairs, https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/pdf/special_event/en/special_event_01.pdf; and World Trade Organization, "Joint Statement on Electronic Commerce," World Trade Organization WT/L/1056, January 25, 2019, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/L/1056.pdf&Open=True.

183 The Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence was adopted in November 2021. See Council of Europe, "Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence," Council of Europe, May 12, 2022, https://rm.coe.int/1680a49dab.

184 U.S. Department of Justice, "CLOUD Act Resources," U.S. Department of Justice, August 17, 2022, https://www.justice.gov/dag/cloudact.

185 United Nations (UN) General Assembly, "Countering the Use of Information and Communications Technologies for Criminal Purposes, Resolution Adopted by the General Assembly," UN General Assembly A/RES/74/247, December 27, 2019, https://digitallibrary.un.org/record/3847855?ln=en.

186 Indian Ministry of Finance, "Data 'of the People by the People, for the People," in *Economic Survey 2018–2019* 1 (2019): 78–97, https://www.indiabudget.gov.in/budget2019-20/economicsurvey/doc/vol1chapter/echap04_vol1.pdf.

187 Indian Ministry of Electronics and Information Technology and Committee of Experts on Non-Personal Data Governance Framework (Gopalakrishnan Committee), "Report by the Committee of Experts on Non-Personal Data Governance Framework," Indian Ministry of Electronics and Information Technology and Gopalakrishnan Committee, December 16, 2020, https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf. An earlier version of the committee's recommendations was put out for public comments in July 2020. See Indian Ministry of Electronics and Information Technology and Gopalakrishnan Committee, "Report by the Committee of Experts on Non-Personal Data Governance Framework," Indian Ministry of Electronics and Information Technology and Gopalakrishnan Committee, 2020, https://ourgovdotin.files.wordpress.com/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf.

188 Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (Srikrishna Committee), *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, (New Delhi: Srikrishna Committee, 2018), https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

189 Lok Sabha, "List of Business," Lok Sabha, August 3, 2022, http://164.100.47.194/Loksabha/Business/ListofBusiness.aspx.

190 Press Trust of India, "Vaishnaw Hopeful of Getting New Data Protection Bill Passed by Budget," *Business Standard*, August 5, 2022, https://www.business-standard.com/article/current-affairs/vaishnaw-hopeful-of-getting-new-data-protection-bill-passed-by-budget-122080400290_1.html.

191 Srikrishna Committee, *A Free and Fair Digital Economy*, 12.

192 See Sections 35 and 91 of the Personal Data Protection Bill, 2019. Both these provisions were retained, with minor modifications, in the joint parliamentary committee's recommendations. Lok Sabha, "The Personal Data Protection Bill, 2019," Lok Sabha, Bill No. 373 of 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

193 Rishab Bailey and Smriti Parsheera, "Data Localization in India: Paradigms and Processes," CSI Transactions on ICT 9, no. 3 (September 2021):137–150, https://doi.org/10.1007/s40012-021-00337-4; Anirudh Burman and Upasana Sharma, "How Would Data Localization Benefit India?," Carnegie India, April 14, 2021, https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-84291; and Arindrajit Basu, Ellonai Hickok, and Aditya Singh Chawla, "The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India," Centre for Internet and Society, March 19, 2019 https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf.

194 Anja Kovacs and Nayantara Ranganathan, "Data Sovereignty, of Whom? Limits and Suitability of Sovereignty Frameworks for Data in India," Data Governance Network Working Paper 3, November 2019, https://datagovernance.org/report/data-sovereignty.

195 Rajat Kathuria, Mansi Kedia, Gangesh Varma, and Kaushambi Bagchi, "Economic Implications of Cross Border Data Flows," Indian Council for Research on International Economic Relations and Internet and Mobile Association of India, November 2019, https://icrier.org/pdf/Economic_Implications_of_Cross-Border_Data_Flows.pdf; Shagufta

Gupta, Kapil Gupta, Poulomi Ghosh, and Sudip Kumar Paul, "Data Localisation: India's Double-Edged Sword?," CUTS International, 2020, https://cuts-ccier.org/pdf/data-localisation-indias-double-edged-sword.pdf; and Sai Rakshith Potluri, V. Sridhar, and Shrisha Rao, "Effects of Data Localization on Digital Trade: An Agent-Based Modeling Approach," *Telecommunications Policy* 44, no. 9 (2020), https://doi.org/10.1016/j.telpol.2020.102022.

196 Smriti Parsheera and Prateek Jha, "Cross-Border Data Access for Law Enforcement: What Are India's Strategic Options?," Carnegie India, November 2020, https://carnegieendowment.org/files/ParsheeraJha_DataAccess.pdf; Madhulika Srikumar, Sreenidhi Srinivasan, DeBrae Kennedy-Mayo, and Peter Swire, "India-US Data Sharing for Law Enforcement: Blueprint for Reforms," Observer Research Foundation and Georgia Tech Institute for Information Security & Privacy's Cross-Border Requests for Data Project, January 17, 2019, https://www.orfonline.org/wp-content/uploads/2019/01/MLAT-Book-_v8_web-1.pdf; Amber Sinha, Elonnai Hickok, Udbhav Tiwari, and Arindrajit Basu, "Cross Border Data-Sharing and India: A Study in Processes, Content and Capacity," Centre for Internet and Society, February 2016, https://cis-india.org/internet-governance/files/mlat-report; and Justin Sherman, "Trading in US-India Data Flows: Prospects for Cooperation in US-India Data Policy," Atlantic Council, March 2022, https://www.atlanticcouncil.org/wp-content/uploads/2022/03/Cross_Border_Data_Flows.pdf.

197 Indian Ministry of Electronics and Information Technology Indian Computer Emergency Response Team (CERT-In), "Directions Under Sub-section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe and Trusted Internet," Indian Ministry of Electronics and Information Technology CERT-In, No. 20(3)/2022-CERT-In, April 28, 2022, https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf.

198 In the case of the Ministry of Health and Family Welfare, this was due to the abandonment of the draft Digital Information Security in Healthcare Act as a whole. The e-commerce data localization issue, on the other hand, ran into troubles of ministerial remit since the subject of data flows falls under the domain of the Ministry of Electronics and Information Technology, not the Ministry of Commerce and Industry, which is the agency that produced the draft of the e-commerce policy. See Asit Ranjan Mishra, "Data Storage Rules Out of e-Commerce Policy," *Live Mint*, June 26, 2019, https://www.livemint.com/politics/policy/data-storage-rules-out-of-e-commerce-policy-1561488393145.html. Indian Ministry of Commerce and Industry Department for Promotion of Industry and Internal Trade, "Draft National e-Commerce Policy: India's Data for India's Development," Indian Ministry of Commerce and Industry Department for Promotion of Industry and Internal Trade, February 23, 2019, https://dpiit.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf; and Indian Ministry of Health and Family Welfare, "Subject: Placing the Draft of 'Digital Information Security in Healthcare, Act (DISHA)" in Public Domain for Comments/Views-Reg," Indian Ministry of Health and Family Welfare," March 21, 2018, https://www.nhp.gov.in/NHPfiles/R_4179_1521627488625_0.pdf.

199 In 2015, India's Department of Telecommunications issued a National Telecom M2M Roadmap stating that there was a "strong case for all M2M Gateways and application servers, servicing the customers in India, to be physically located in India" for security reasons. See Indian Ministry of Communications Department of Telecommunications, "National Telecom M2M Roadmap," Indian Ministry of Communications Department of Telecommunications, May 2015, https://web.archive.org/web/20220305194717/https://dot.gov.in/sites/default/files/National%20Telecom%20M2M%20Roadmap.pdf.

200 Bailey and Parsheera, "Data Localization in India: Paradigms and Processes"; Rishab Bailey and Smriti Parsheera, "Data Localisation in India: Questioning the Means and Ends," National Institute of Public Finance and Policy Working Paper No. 242, September 2018, https://www.nipfp.org.in/media/medialibrary/2018/10/WP_2018_242.pdf; Christopher Kuner, "Data Nationalism and Its Discontents," *Emory Law Journal* 64 (2015): 2089, https://scholarlycommons.law.emory.edu/elj-online/25/; and Anupam Chander and Uyên P. Lê, "Data Nationalism," *Emory Law Journal 64* (2015): 677, https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2/.

201 See Paragraph 3.11.2. Survey of India, "National Geospatial Policy," Survey of India, July 11, 2021, https://www.surveyofindia.gov.in/webroot/UserFiles/files/NGP_11_07_Draft.pdf.

202 Basu, Hickok, and Chawla," The Localisation Gambit," 48–49.

203 Ibid., 49.

204 Ibid.

205 Srikrishna Committee, *A Free and Fair Digital Economy*, 84–86.

206 D Y Chandrachud, "Justice K.S. Puttaswamy (Retd) v. Union of India and Ors.," Indian Kanoon (Indian Supreme Court Writ Petition (Civil) No. 494 of 2012) 2012, https://indiankanoon.org/doc/91938676.

207 For further discussion on the Puttaswamy tests, see Vrinda Bhandari, Amba Kak, Smriti Parsheera, and Faiza Rahman, "An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict," Leap Blog, September 20, 2017, https://blog.theleapjournal.org/2017/09/an-analysis-of-puttaswamy-supreme.html.

208 The Srikrishna Committee's report, however, dismisses this concern on the grounds that censorship is not an automatic consequence of local retention and would only be possible with a dysfunctional data protection law that allows governments the tools to facilitate such censorship. See Srikrishna Committee, *A Free and Fair Digital Economy*, 95.
209 "22 YouTube Channels Blocked Over 'Anti-India'Content," *Indian Express*, April 5, 2022, https://indianexpress.com/article/india/govt-blocks-youtube-channels-anti-india-7853880.
210 Bailey and Parsheera, "Data Localization in India: Paradigms and Processes", 141.
211 Thomas K. Thomas, "National Security Council Proposes 3-Pronged Plan to Protect Internet Users," *Hindu*, February 13, 2014, https://www.thehindubusinessline.com/info-tech/National-Security-Council-proposes-3-pronged-plan-to-protect-Internet-users/article20727012.ece.
212 Srikrishna Committee, *A Free and Fair Digital Economy*, 92–93.
213 Reserve Bank of India, "Statement on Developmental and Regulatory Policies," Reserve Bank of India, April 5, 2018, https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=43574.
214 Reserve Bank of India, "Storage of Payment System Data," Reserve Bank of India, 2018, https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244.
215 The recommendations link the requirements on local data storage with the sensitivity attached to the underlying personal data. This may suggest that nonpersonal data that is not derived from personally identifiable information would not be subject to any cross-border flow restrictions, though the committee has not made this clear.
216 Joint Parliamentary Committee, *Report of the Joint Committee on the Personal Data Protection Bill, 2019*, 40.
217 Reserve Bank of India, "Storage of Payment System Data," paragraph 2.
218 This is preceded by a requirement that the outsourcing of activities to entities abroad is subject to the laws and regulations of that jurisdiction not impeding regulatory access and oversight by the Insurance Regulatory and Development Authority of India. Insurance Regulatory and Development Authority of India (IRDAI), "Outsourcing of Activities by Indian Insurers Regulations, 2017," IRDAI, April 20, 2017, 13, https://www.irdai.gov.in/admincms/cms/frmGeneral_Layout.aspx?page=PageNo3149&flag=1.
219 Indian Ministry of Electronics and Information Technology CERT-In, "Directions Under Sub-section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe and Trusted Internet."
220 The Srikrishna Committee noted that critical data in this context may well extend beyond personal data to include things like information relating to government services or the country's critical infrastructure. See Srikrishna Committee, *A Free and Fair Digital Economy*, 91.
221 Bailey and Parsheera, "Data Localization in India: Paradigms and Processes," 145–146.
222 Securities and Exchange Board of India, "Annexure A, CERT Fin Advisory 201155100308, Advisory for Financial Sector Organizations - RBI and SEBI," Securities and Exchange Board of India, 2020, https://web.archive.org/web/20211015204605/https://www.sebi.gov.in/sebi_data/commondocs/nov-2020/Annexure%20A_p.pdf.
223 See Paragraph 6.5 of India's National Data Sharing and Accessibility Policy. See Indian Ministry of Science and Technology Department of Science and Technology, "National Data Sharing and Accessbility Policy-2012 (NDSAP-2012)," Indian Ministry of Science and Technology Department of Science and Technology, 2012, 5, https://geoportal.mp.gov.in/geoportal/Content/Policies/NDSAP_2012.pdf.
224 See Paragraph 8.1 of the Gopalakrishnan Committee's report. See Gopalakrishnan Committee, "Report by the Committee of Experts on Non-Personal Data Governance Framework," 23.
225 See Appendix 2 of the Gopalakrishnan Committee's report. See Gopalakrishnan Committee, "Report by the Committee of Experts on Non-Personal Data Governance Framework," 38–43.
226 Joint Parliamentary Committee, "Report of the Joint Committee on the Personal Data Protection Bill, 2019," 9.
227 This is in addition to the jobs generated during the project's construction phase, a figure estimated at 28,696 jobs. See Joint Parliamentary Committee, "Report of the Joint Committee on the Personal Data Protection Bill, 2019," 41.
228 Swathi Moorthy and Chandra R Srikanth, "Indian IT Industry Crosses $200 Billion in Revenue With 5 Million Direct Employees," Money Control, February 15, 2022, https://www.moneycontrol.com/news/opinion/indian-it-industry-crosses-200-billion-in-revenue-with-5-million-direct-employees-8099841.html.
229 Bailey and Parsheera, "Data Localisation in India: Questioning the Means and Ends," 31.
230 See Section 91(2) of the Personal Data Protection Bill, 2019, and Section 92(2) of the 2021 DP Bill.
231 Gopalakrishnan Committee, "Report by the Committee of Experts on Non-Personal Data Governance Framework," 23–24, 29–30.
232 Zachary Oliver, Kyle Clark-Sutton, Sara VanLear, Lindsay Aramayo, and Brian Lim et al., "The Impact of Facebook's U.S. Data Center Fleet," RTI International, March 2018, https://baxtel.com/data-center/facebook/files/facebook_data_centers_2018.

233 Ibid.
234 While announcing its new cloud platform region in Mumbai, Google declared that this would improve latency from 20 percent to 90 percent for end users in certain Indian cities compared to hosting these services in Singapore, which was the closest region. See Dave Stiver, "GCP Arrives in India With Launch of Mumbai Region," Google Cloud, November 1, 2017, https://cloud.google.com/blog/products/gcp/gcp-arrives-in-india-with-launch-of-mumbai-region.
235 Shamel Azmeh and Christopher Foster, "The TPP and the Digital Trade Agenda: Digital Industrial Policy and Silicon Valley's Influence on New Trade Agreements," London School of Economics, Working Paper Series No. 16-175, 2016, http://hdl.handle.net/10419/224801.
236 Mitaksh, "Data Protection Bill: Restrictions on Cross-Border Data Transfer Will Hurt Indian Start-ups That Depend on Global Tools #NAMA," Medianama, January 27, 2022, https://www.medianama.com/2022/01/223-cross-border-data-transfer-small-business.
237 Srikrishna Committee, *A Free and Fair Digital Economy*, 94.
238 Bailey and Parsheera, "Data Localization in India: Paradigms and Processes," 148.
239 Kathuria, Kedia, Varma, and Bagchi, "Economic Implications of Cross Border Data Flows," 29.
240 Burman and Sharma, "How Would Data Localization Benefit India?."
241 Sebastian Moss, "India's Data Center Market Heats Up," Data Center Dynamics, October 7, 2021, https://www.datacenterdynamics.com/en/analysis/indias-data-center-market-heats-up.
242 Indian Ministry of Electronics and Information Technology e-Governance Division, "Data Centre Policy 2020," Indian Ministry of Electronics and Information Technology e-Governance Division, 2020, https://web.archive.org/web/20220310202706/https://www.meity.gov.in/writereaddata/files/Draft%20Data%20Centre%20Policy%20-%2003112020_v5.5.pdf.
243 Vandana Ramnani, "Budget 2022: Data Centres to Be Given Infrastructure Status to Boost Financing of Sector," Money Control, February 1, 2022, https://www.moneycontrol.com/news/business/real-estate/budget-2022-data-centres-to-be-given-infrastructure-status-8018221.html.
244 Japanese Ministry of Foreign Affairs, "Osaka Declaration on Digital Economy."
245 See Paragraphs 10 and 11 of the following G20 declaration. See Japanese Ministry of Foreign Affairs, "G20 Osaka Leaders' Declaration," Japanese Ministry of Foreign Affairs, 2019, https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html#:~:text=We%2C%20the%20Leaders%20of%20the,for%20the%20benefit%20of%20all.
246 Japanese Ministry of Foreign Affairs, "Osaka Declaration on Digital Economy"; and Prerna Gandhi, "Review of Japan 2019 and Outlook for 2020," Vivekananda International Foundation, February 3, 2020, http://manage.vifindia.org/print/7087.
247 Ibid.
248 Indian Ministry of Commerce and Industry, "Shri Piyush Goyal Participates in the G-20 Meeting of the Trade and Investment Ministers," Indian Press Information Bureau, September 22, 2020, https://pib.gov.in/PressReleasePage.aspx?PRID=1657874; and Indian Ministry of External Affairs, "G20 Sherpa, Shri Piyush Goyal Holds Special Briefing From Rome," Indian Ministry of External Affairs, October 30, 2021, https://www.mea.gov.in/press-releases.htm?dtl/34444/G20+Sherpa+Shri+Piyush+Goyal+holds+Special+Briefing+from+Rome.
249 D. Ravi Kanth, "India Boycotts 'Osaka Track' at G20 Summit," *Live Mint*, June 30, 2019, https://www.livemint.com/news/world/india-boycotts-osaka-track-at-g20-summit-1561897592466.html; and Indian Ministry of External Affairs, "Transcript of Media Briefing by Foreign Secretary After BRICS Leaders' Informal Meeting in Osaka," Indian Ministry of External Affairs, June 28 2019, https://www.mea.gov.in/media-briefings.htm?dtl/31516/Transcript_of_Media_Briefing_by_Foreign_Secretary_after_BRICS_Leaders_Informal_meeting_in_Osaka.
250 World Trade Organization, "Joint Initiative on E-commerce," World Trade Organization, https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm.
251 World Trade Organization (Statement by India and South Africa), "The Legal Status of 'Joint Statement Initiatives' and Their Negotiated Outcomes," World Trade Organization, February 19, 2021, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/GC/W819.pdf&Open=True.
252 Indian Ministry of Commerce and Industry, "India's Stand in the WTO: Statement in Parliament," Statement by Shri Suresh Prabhu, Minister of Commerce and Industry after the Eleventh Ministerial Conference of the World Trade Organization held in Buenos Aires, Argentina, December 2017, https://commerce.gov.in/wp-content/uploads/2020/11/Flag-L_CIM-statement-in-Parliament-after-MC-11.pdf.
253 World Trade Organization (Statement by India and South Africa), "The Legal Status of 'Joint Statement Initiatives' and Their Negotiated Outcomes."
254 Indian Ministry of Commerce and Industry, "India's Stand in the WTO," 5.
255 Indian Prime Minister's Office, "Joint Statement on BRICS Leaders' Informal Meeting on the Margins of G20 Summit," Press Information Bureau, June 28, 2019, https://pib.gov.in/PressReleseDetail.aspx?PRID=1576270.

256 Group of 77, "About the Group of 77," Group of 77, https://www.g77.org/doc/index.html.
257 Group of 77, "Ministerial Declaration (adopted by the 45th Annual Meeting of Ministers for Foreign Affairs of the Group of 77)," Group of 77, November 30, 2021, https://www.g77.org/doc/Declaration2021.htm.
258 Arindrajit Basu, "The Retreat of the Data Localization Brigade: India, Indonesia and Vietnam," *Diplomat*, January 10, 2020, https://thediplomat.com/2020/01/the-retreat-of-the-data-localization-brigade-india-indonesia-and-vietnam.
259 See Article 9.11 in the Comprehensive Economic Partnership Agreement (CEPA) between India and the United Arab Emirates (UAE). Indian Ministry of Commerce and Industry, "Chapter 9: Digital Trade," Indian Ministry of Commerce and Industry, https://commerce.gov.in/wp-content/uploads/2022/03/Chapter-9.pdf.
260 See Article 9.3(4) of the CEPA between India and the UAE. Indian Ministry of Commerce and Industry, "Chapter 9: Digital Trade."
261 Kritika Sunej, "India May Get Access to $10-billion Australian Government Tenders," *Economic Times*, April 4, 2022, https://economictimes.indiatimes.com/news/economy/foreign-trade/india-may-get-access-to-10-billion-australian-government-tenders/articleshow/90631268.cms.
262 World Trade Organization, "E-commerce Co-Convenors Welcome Substantial Progress in Negotiations," World Trade Organization, December 14, 2021, https://www.wto.org/english/news_e/news21_e/ecom_14dec21_e.htm.
263 Basu, "The Retreat of the Data Localization Brigade: India, Indonesia and Vietnam."
264 Akshay Mathur and Purvaja Modak, "Goodbye, RCEP," Gateway House, November 7, 2019, https://web.archive.org/web/20210509035604/https://www.gatewayhouse.in/rcep/.
265 Indian Ministry of External Affairs, "G20 Sherpa, Shri Piyush Goyal Holds Special Briefing From Rome."
266 Rishab Bailey, Vrinda Bhandari, Smriti Parsheera, and Faiza Rahman, "Use of Personal Data by Intelligence and Law Enforcement Agencies," National Institute of Public Finance and Policy, August 1, 2018, https://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data.pdf.
267 See Section 91 of the Code of Criminal Procedure, 1973. India Code, "The Code of Criminal Procedure, 1973," India Code, 1973, https://www.indiacode.nic.in/handle/123456789/16225?sam_handle=123456789/1362.
268 See Section 5 of the Indian Telegraph Act, 1885. See Indian Ministry of Communications Department of Telecommunications, "Indian Telegraph Act, 1885," Indian Ministry of Communications Department of Telecommunications, 1885, https://dot.gov.in/sites/default/files/the_indian_telegraph_act_1985_pdf.pdf. Also see Section 69 of the Information Technology Act, 2000. India Code, "Information Technology Act, 2000," India Code, 2000, https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf. For further information, see Bailey, Bhandari, Parsheera, and Rahman, "Use of Personal Data by Intelligence and Law Enforcement Agencies."
269 Parsheera and Jha, "Cross-Border Data Access for Law Enforcement."
270 Joint Parliamentary Committee, "Report of the Joint Committee on the Personal Data Protection Bill, 2019," 8.
271 See Rule 4(2) of the "Information Technology (Intermediary Guidelines and Digital Media Ethics Code), 2021." See Indian Ministry of Electronics and Information Technology, "Information Technology (Intermediary Guidelines and Digital Media Ethics Code), 2021," Indian Ministry of Electronics and Information Technology, February 25, 2021, https://web.archive.org/web/20220310204124/https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf; and Prasid Banerjee and Richa Banka, "WhatsApp Case in Delhi HC First Big Test of Privacy Law," *Live Mint*, May 27, 2021, https://www.livemint.com/news/india/whatsapps-case-against-indian-govt-could-be-first-true-test-of-right-to-privacy-11622028707630.html.
272 Indian Press Information Bureau, "Centralised System to Monitor Communication," Indian Press Information Bureau, November 26, 2009, http://pib.nic.in/newsite/PrintRelease.aspx?relid= 54679.
273 Internet Freedom Foundation, "Watch the Watchmen Series, Part 2: The Centralised Monitoring System," September 14, 2020, https://internetfreedom.in/watch-the-watchmen-series-part-2-the-centralised-monitoring-system. Also see Bailey, Bhandari, Parsheera, and Rahman, "Use of Personal Data by Intelligence and Law Enforcement Agencies," 12.
274 "Why Five Petitions Are Challenging the Constitutional Validity of India's Surveillance State," *Wire*, January 14, 2019, https://thewire.in/law/supreme-court-pil-centre-snooping.
275 Parsheera and Jha, "Cross-Border Data Access for Law Enforcement."
276 Press Trust of India, "Received 40,300 Govt Requests for User Data From India: Facebook Report," *Hindustan Times*, May 20, 2021, https://www.hindustantimes.com/india-news/received-40-300-govt-requests-for-user-data-from-india-facebook-report-101621505028130.html.
277 Letters rogatory can be issued under Section 166A and Section 105K of the Code of Criminal Procedure, 1973; Section 57 and Section 61 of the Prevention of Money Laundering Act, 2002; and Section 12 of the Fugitive Economic Offenders Act, 2018. See Indian Ministry of Home Affairs, "Guidelines on Mutual Legal Assistance in Criminal Matters," Indian Ministry of Home Affairs, December 5, 2019 https://web.archive.org/web/20211117011824/https://www.mha.gov.in/sites/default/files/ISII_ComprehensiveGuidelines16032020.pdf.

278 Indian Ministry of Home Affairs, "Guidelines on Mutual Legal Assistance in Criminal Matters," 4.
279 This information was submitted before the committee by the Ministry of Home Affairs. See Lok Sabha Parliamentary Committee on External Affairs, "Report of the Committee on External Affairs (2020-21) on India and International Law Including Extradition Treaties With Foreign Countries, Asylum Issues, International Cyber-Security and Issues of Financial Crimes," Lok Sabha Parliamentary Committee on External Affairs, 13, https://web.archive.org/web/20211203114141/http://164.100.47.193/lsscommittee/External%20Affairs/17_External_Affairs_9.pdf.
280 Ibid.
281 Neha Alawadhi, "CBI and FBI Join Hands to Reduce Time Required to Fulfil Requests on Information and Evidence," *Economic Times*, December 7, 2015, https://economictimes.indiatimes.com/news/politics-and-nation/cbi-fbi-join-hands-to-reduce-time-required-to-fulfil-requests-on-information-and-evidence/articleshow/50069794.cms.
282 Lok Sabha Parliamentary Committee on External Affairs, "Report of the Committee on External Affairs (2020-21) on India and International Law Including Extradition Treaties With Foreign Countries, Asylum Issues, International Cyber-Security and Issues of Financial Crimes," 16.
283 Indian Ministry of Home Affairs, "Guidelines on Mutual Legal Assistance in Criminal Matters," 4.
284 Lok Sabha Parliamentary Committee on External Affairs, "Report of the Committee on External Affairs (2020-21) on India and International Law Including Extradition Treaties With Foreign Countries, Asylum Issues, International Cyber-Security and Issues of Financial Crimes."
285 Indian Ministry of Home Affairs, "Guidelines on Mutual Legal Assistance in Criminal Matters."
286 Basu, Hickok, and Chawla, "The Localisation Gambit"; Burman and Sharma, "How Would Data Localization Benefit India?"; and Parsheera and Bailey, "Data Localization in India: Paradigms and Processes."
287 Monika Zalnieriute, "Big Brother Watch and Others V. the United Kingdom," American Journal of International Law 116, no. 3 (July 2022): 585–592, https://www.cambridge.org/core/journals/american-journal-of-international-law/article/big-brother-watch-and-others-v-the-united-kingdom/024BF9DDDFA0C882358B052845230352.
288 Lok Sabha Parliamentary Committee on External Affairs, "Report of the Committee on External Affairs (2020-21) on India and International Law Including Extradition Treaties With Foreign Countries, Asylum Issues, International Cyber-Security and Issues of Financial Crimes," 29.
289 7amleh - The Arab Center for the Advancement of Social Media, Access Now, Africa Freedom of Information Centre, Albanian Media Institute, and Americans for Democracy and Human Rights in Bahrain et al., "Open Letter to UN General Assembly: Proposed International Convention on Cybercrime Poses a Threat to Human Rights Online," Association for Progressive Communications, November 6, 2019, https://www.apc.org/en/pubs/open-letter-un-general-assembly-proposed-international-convention-cybercrime-poses-threat-human.
290 Lok Sabha Parliamentary Committee on External Affairs, "Report of the Committee on External Affairs (2020-21) on India and International Law Including Extradition Treaties With Foreign Countries, Asylum Issues, International Cyber-Security and Issues of Financial Crimes," 30.
291 Ibid., 45.
292 Ibid., 29.
293 Soumyarendra Barik, "Why ExpressVPN Has Removed Its Servers From India, and What Happens to Users Now," *Indian Express*, June 2, 2022, https://indianexpress.com/article/explained/expressvpn-services-india-new-vpn-rules-explained-7948845.
294 Indian Ministry of External Affairs, "G20 Sherpa, Shri Piyush Goyal Holds Special Briefing From Rome."
295 Parsheera and Jha, "Cross-Border Data Access for Law Enforcement."
296 Ibid.
297 Ibid., 25.
298 IRDAI, "Outsourcing of Activities by Indian Insurers Regulations, 2017."
299 Ibid. See Regulation 18(ii).
300 Reserve Bank of India, "Storage of Payment System Data."
301 Reserve Bank of India, "Frequently Asked Questions: Storage of Payment System Data," Reserve Bank of India, April 6, 2018, https://m.rbi.org.in/scripts/FAQView.aspx?Id=130.
302 Reserve Bank of India, "Storage of Payment System Data." See Paragraph 2(1).
303 Bailey and Parsheera, "Data Localization in India: Paradigms and Processes," 144.
304 Reserve Bank of India, "Amendment to the Master Direction (MD) on KYC," Reserve Bank of India, May 10, 2021, https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT354BE2BCC23B344982BD5793737940EFF3.PDF.
305 See 39.23 (vi), Chapter 1, Part IV of the License Agreement for Unified License. See Indian Ministry of Communications and Information Technology Department of Telecommunications, "License Agreement for Unified License," Indian Ministry of Communications and Information Technology Department of Telecommunications, https://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf. A similar provision appears in the Unified Access Service License.

306 Ibid.
307 See Annexure 6, Condition 1.3(ix) of the Consolidated FDI Policy. See Indian Ministry of Commerce and Industry, Department for Promotion of Industry and Internal Trade, "Consolidated FDI Policy," Indian Ministry of Commerce and Industry, Department for Promotion of Industry and Internal Trade, October 15, 2020, https://dpiit.gov.in/sites/default/files/FDI-PolicyCircular-2020-29October2020.pdf.
308 Ibid.
309 See Proviso to Rule 3(2)(5). See Indian Ministry of Corporate Affairs, "Notification: G.S.R.239," Indian Ministry of Corporate Affairs, March 31, 2014, https://www.mca.gov.in/Ministry/pdf/NCARules_Chapter9.pdf.
310 Ibid.
311 Securities and Exchange Board of India, "Advisory for Financial Sector Organizations Regarding Software as a Service (SaaS) Based Solutions," Securities and Exchange Board of India, November 3, 2020, https://www.sebi.gov.in/legal/circulars/nov-2020/advisory-for-financial-sector-organizations-regarding-software-as-a-service-saas-based-solutions_48081.html. The advisory by CERT-In is included as an annexure to this circular. See Securities and Exchange Board of India, "Annexure A: CERT-Fin Advisory – 201155100308: Advisory for Financial Sector Organisations – RBI and SEBI," Securities and Exchange Board of India, November 3, 2020, https://www.sebi.gov.in/sebi_data/commondocs/nov-2020/Annexure%20A_p.pdf.
312 National Archives of India, "Public Records Act, 1993," National Archives of India, 1993, http://nationalarchives.nic.in/content/public-records-act-1993-0.
313 Ibid., Section 4.
314 Indian Department of Electronics and Information Technology, "Request for Proposal for Provisional Empanelment of Cloud Service Providers," Indian Department of Electronics and Information Technology, December 30, 2015, https://web.archive.org/web/20220302220806/https://www.meity.gov.in/writereaddata/files/RFP_CSPs_10_16.pdf; and Indian Ministry of Electronics and Information Technology, "Guidelines for Government Departments on Contractual Terms Related to Cloud Services," Indian Ministry of Electronics and Information Technology, March 31, 2017, https://web.archive.org/web/20220608195421/https://www.meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms.pdf.
315 Indian Department of Electronics and Information Technology, "Request for Proposal for Provisional Empanelment of Cloud Service Providers," Clause 5.7(2).
316 Indian Ministry of Science and Technology Department of Science and Technology, "National Data Sharing and Accessibility Policy-2012 (NDSAP-2012)," Indian Ministry of Science and Technology Department of Science and Technology, 2012, https://geoportal.mp.gov.in/geoportal/Content/Policies/NDSAP_2012.pdf.
317 (CERT-In), "Directions Under Sub-section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe and Trusted Internet."
318 Ibid., 3.
319 Indian Ministry of Electronics and Information Technology (CERT-In), "Extension of Timelines for Enforcement of Cyber Security Directions of 28th April, 2022," Indian Ministry of Electronics and Information Technology (CERT-In), June 27, 2022, https://web.archive.org/web/20220701155342/https://www.cert-in.org.in/PDF/CERT-In_directions_extension_MSMEs_and_validation_27.06.2022.pdf.
320 Indian Ministry of Communications and Information Technology, "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011," Indian Ministry of Communications and Information Technology, April 11, 2011, https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf.
321 Ibid., Rule 7.
322 Lok Sabha, "Personal Data Protection Bill, 2019."
323 Gopalakrishnan Committee, "Report by the Committee of Experts on Non-Personal Data Governance Framework."
324 Ibid., 31.
325 Indian Ministry of Health and Family Welfare, "Digital Information Security in Healthcare Act [Draft for Public Consultation]," Indian Ministry of Health and Family Welfare,
November 2017, https://www.nhp.gov.in/NHPfiles/R_4179_1521627488625_0.pdf.
326 Ibid., Section 22(1)(e).
327 Indian Ministry of Health and Family Welfare Central Drugs Standard Control Organization, "Draft Drugs and Cosmetics (Amendment) Rules, 2018," Indian Ministry of Health and Family Welfare Central Drugs Standard Control Organization, August 28, 2018, https://cdsco.gov.in/opencms/opencms/system/modules/CDSCO.WEB/elements/download_file_division.jsp?num_id=MTkzOQ==.
328 Ibid., Rule 67K(3).

329 Indian Ministry of Commerce and Industry Department for Promotion of Industry and Internal Trade, "Draft National e-Commerce Policy."
330 Ibid., 16.
331 Survey of India, "National Geospatial Policy."
332 Ibid., Paragraph 7.2.10.

Chapter 4

333 Young-tae Oh, "Rep. Jae-il Byun Proposes a Bill to Resolve Discrimination Against Global IT Companies," *News Prime*, September 4, 2018, http://www.newsprime.co.kr/news/article/?no=428794.
334 Asia-Pacific Economic Cooperation, "What Is the Cross-Border Privay Rules System," Asia-Pacific Economic Cooperation, October 2021, https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system.
335 Michael Kwet, "Digital Colonialism Is Threatening the Global South," Al Jazeera, March 13, 2019, https://www.aljazeera.com/opinions/2019/3/13/digital-colonialism-is-threatening-the-global-south.
336 Park Ji-sung, "[Issue Analysis] Global CP - Resolving Reverse Discrimination Against Domestic Companies, Remaining Tasks," *ET News*, May 8, 2020, https://m.etnews.com/20200507000287.
337 Anupam Chander and Haochen Sun, "Sovereignty 2.0," Georgetown Law Faculty Publications and Other Works, August 10, 2021, 8, https://scholarship.law.georgetown.edu/facpub/2404.
338 For an objective genealogy of China's conceptions of data sovereignty, see Chander and Sun, "Sovereignty 2.0."
339 Adrian Shabaz, Allie Funk, and Andrea Hackl, "User Privacy or Cyber Sovereignty: Assessing the Human Rights Implications of Data Localization," Freedom House, 2020, https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty.
340 Julia Yoon, "South Korean Data Localization: Shaped by Conflict," University of Washington's Henry M. Jackson School of International Studies, February 28, 2018, https://jsis.washington.edu/news/south-korean-data-localization-shaped-conflict.
341 Rich Miller, "Germany's Merkel Calls for Separate European Internet," DataCenterKnowledge.com, February 14, 2017, https://www.datacenterknowledge.com/archives/2014/02/17/germanys-merkel-calls-separate-european-internet; and Albright Stonebridge Group, "Data Localization: A Challenge to Global Commerce and the Free Flow of Information," September 2015, 8, https://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20-%20September%202015.pdf.
342 Law360, "Brazil Nixes Data Localization Mandate From Internet Bill," Law360, March 20, 2014, https://www.law360.com/articles/520198/brazil-nixes-data-localization-mandate-from-internet-bill.
343 Surabhi Agarwal and Megha Mandavia, "Local Servers of Tech Giants Like Facebook, Google May Help Indian Govt Debit Taxes, *Economic Times, December 17, 2018,* https://telecom.economictimes.indiatimes.com/news/local-servers-of-tech-giants-like-facebook-google-may-help-indian-govt-debit-taxes/67121723.
344 Jennifer Rankin, "EU to Find Ways to Make Google, Facebook and Amazon Pay More Tax, *Guardian,* September 21, 2017, https://www.theguardian.com/business/2017/sep/21/tech-firms-tax-eu-turnover-google-amazon-apple.
345 "Indonesia May Force Web Giants to Build Local Data Centers," *Asia Sentinel, January 17, 2014,* https://www.asiasentinel.com/p/indonesia-web-giants-local-data-centers.
346 Martin Schulz, "Keynote Speech at CPDP2016 on Technological, Totalitarianism, Politics and Democracy," Lexxion 2 (2016): 11–14 https://edpl.lexxion.eu/article/edpl/2016/1/4/display/html.
347 Philippe Bradley and Mark Young, "EU Data Retention Directive Declared Invalid by Court of Justice of the EU," *Inside Privacy, April 8, 2014,* https://www.insideprivacy.com/international/european-union/eu-data-retention-directive-declared-invalid-by-court-of-justice-of-the-eu.
348 Chander and Sun, "Sovereignty 2.0," 24–25.
349 Lee Kyung-min, "'Google Tax' Emerges as Korea-US Trade Issue," *Korea Times*, December 10, 2018, https://www.koreatimes.co.kr/www/biz/2018/12/602_260148.html; Oh, "Rep. Jae-il Byun Proposes a Bill to Resolve Discrimination Against Global IT Companies"; Minji Choi, "Global CP Reverse Discrimination Relief Act, A Record of the Day," *Digital Daily*, May 17, 2020, http://m.ddaily.co.kr/m/m_article/?no=195657; Lee Doo-hyun, "Will the 'Google Tax,' Problem Be Solved? Rep. Jae-il Byun Proposes a Bill to Resolve Reverse Discrimination," *Inven*, September 5, 2018, https://m.inven.co.kr/webzine/wznews.php?l=184805&p=298&idx=206539; Kwon Min-soo, "Reverse Discrimination Between Google, Facebook, Netflix, and Korean IT Companies Will Decrease," *Daily Impact*, https://www.dailyimpact.co.kr/news/articleView.html?idxno=49376; and Park, "[Issue Analysis] Global CP - Resolving Reverse Discrimination Against Domestic Companies, Remaining Tasks."

350 Lalitesh Kathragadda and Arghya Sengupta, "A Digital Dandi March: Push Data Localisation to Preserve Sovereignty and Enable Fair Competition," *Times of India, December 3, 2018,* https://timesofindia.indiatimes.com/blogs/toi-edit-page/a-digital-dandi-march-push-data-localisat.

351 Ireland is the only Council of Europe member that is not a party to the Budapest Convention. Dublin has signed the convention but has not yet ratified it. See Council of Europe, "Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY," Council of Europe, https://www.coe.int/en/web/cybercrime/parties-observers.

352 U.S. Department of Justice Office of Justice Programs, "Criminological Aspects of Economic Crime – Conference of Directors of Criminalogical Research Institutes, 12th, Strasbourg, 15–18 November 1976," U.S. Department of Justice Office of Justice Programs, 1976, https://www.ojp.gov/ncjrs/virtual-library/abstracts/criminological-aspects-economic-crime-conference-directors

353 Council of Europe Committee of Ministers, "Recommendation No. R (89) 9 of the Committee of Ministers to Member States on Computer-Related Crime," Council of Europe Committee of Ministers, September 13, 1989, https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2; and European Committee on Crime Problems, "Report on Computer-related Crime," European Committee on Crime Problems, 1990, (Strasbourg).

354 Council of Europe Committee of Ministers, "Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology," Council of Europe Committee of Ministers, September 11, 1995, https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1900870&SecMode=1&DocId=528034&Usage=2.

355 Council of Europe, "Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems," Council of Europe, European Treaty Series No.189, 2003, https://rm.coe.int/168008160f; and Council of Europe Cybercrime Convention Committee, "Guidance Notes," Council of Europe Cybercrime Convention Committee, December 2012, https://www.coe.int/en/web/cybercrime/guidance-notes.

356 Taejin Chung and Guangmeen Lee, "A Study on Accession by South Korea to the Budapest Convention on Cybercrime and International Cooperation Against Cybercrime," National Police University Institute of Public Security Policy 14, no. 2 (2019): 65–84, https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002469538.

357 Jaejoon Jung, "Plan For Reactions Against International Cyber Crime - Budapest Convention on Cyber Crime Ten Years After Its Adoption," *Contemporary Review of Criminal Law* 39 (June 2013) 6, https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART001778345.

358 Kwang-hyun Ra and Hea-Sung Yoon, "An Empirical Review of the Performance of the Council of Europe Convention against Cybercrime," *Criminal Investigation Studies* 8 (2019) https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE08748900. Also see Council of Europe Cybercrime Convention Committee, "T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime," Europe Cybercrime Convention Committee, December 3, 2014, https://rm.coe.int/16802e726c; and UN Office on Drugs and Crime, "Comprehensive Study on Cybercrime" UN Office on Drugs and Crime, February 2013, https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

359 Heeyoung Park, Hojin Choe, and Sungjin Choe, "Laws Implementing the Cybercrime Treaty," Supreme Prosecutors' Office, 2015, 2–3.

360 Park, Choe, and Choe, "Laws Implementing the Cybercrime Treaty," 129.

361 Korean Constitutional Court, "Case on Location Tracing Data Under Protection of Communications Secrets Act," Korean Constitutional Court, June 28, 2018, http://search.ccourt.go.kr/xmlFile/0/010400/2018/pdf/e2012m191_1.pdf.

362 Korean Legislation Research Institute's Korea Law Translation Center, "Protection of Communications Secrets Act," Korean Legislation Research Institute's Korea Law Translation Center, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=7235&lang=ENG. See Article 13, Paragraph 2.

363 Park, Choe, and Choe, "Laws Implementing the Cybercrime Treaty," 79, 232–236.

364 Hyuk-doo Choi, "A Review on Implementing Legislation for the Adoption of the Cybercrime Convention," National Police University Institute of Public Security Policy 32, no. 3 (December 2018): 387, https://www.dbpia.co.kr/Journal/articleDetail?nodeId=NODE09008821.

365 Chung and Lee, "A Study on Accession by South Korea to the Budapest Convention on Cybercrime and International Cooperation Against Cybercrime"; and Choi, A Review on Implementing Legislation for the Adoption of the Cybercrime Convention," 387.

366 Shin-woo Shin and Do-hee Kim, "Status of Ratification of the Convention on Cybercrime and Korea's Legislative and Policy Responses," National Assembly Research Services, December 2012, 6, https://www.nars.go.kr/report/view.do?cmsCode=CM0158&brdSeq=32493.

367 Korean Legislation Research Institute's Korea Law Translation Center, "Protection of Communications Secrets Act." See Article 15-2, Paragraph 1.

368 Shin and Do-hee Kim, "Status of Ratification of the Convention on Cybercrime and Korea's Legislative and Policy Responses"; and Korean Legislation Research Institute's Korea Law Translation Center, "Telecommunications Business Act," Korean Legislation Research Institute's Korea Law Translation Center, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=59855&lang=ENG.

369 Seon-sik Kim, "User Data No Longer Provided to Investigatory Authorities," *Hankyoreh*, November 1, 2012, https://www.hani.co.kr/arti/economy/economy_general/558613.html.

370 Korean Supreme Court, "Violation of the National Security Act (Praise, Encouragement, etc.), Violation of the National Security Act (Meetings, Communication, etc.)," Korean Supreme Court, Judgment, 2017 Do 9747, November 29, 2017, https://www.law.go.kr/%ED%8C%90%EB%A1%80/(2017%EB%8F%849747).

371 Kyung-lyul Lee and Gunwoo Ha, "A Study on the Implementation of the Budapest Convention on Cybercrime," *Korean Journal of Comparative Criminal Law* 19, no. 4 (2018): 501–534, https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002312731. See pages 524–525.

372 Kim Hankyun, Sung Eun-kim, and Seung Hyun-lee, "International Cooperation for Prevention of Cybercrimes With a Focus on the European Cybercrime Prevention Treaty," Supreme Prosecutors' Office, December 2008, 8–139.

373 Chung and Lee, "A Study on Accession by South Korea to the Budapest Convention on Cybercrime and International Cooperation Against Cybercrime," 78.

374 Lee and Ha, "A Study on the Implementation of the Budapest Convention on Cybercrime," 523.

375 Taehee Han, "[Exclusive] Police Strengthen International Cooperation on Cybercrime . . . Start of Joining the 'Budapest Convention,'" *NewsPim*, June 24, 2020, https://www.newspim.com/news/view/20200623000783.

376 Park Ji-eun, "International Cooperation Is Essential to Track 'Nth Room . . . 'You Must Join the Budapest Convention," *Women News*, April 4, 2020, https://www.womennews.co.kr/news/articleView.html?idxno=197666.

377 Kyung Sin "KS" Park, "Communication Surveillance in Korea" Korea University Law Review 16–17 (May 2015), 53–72, https://ssrn.com/abstract=2748318.

378 Ibid.

379 Ibid.

380 Se Young Lee and Sohee Kim, "South Korea Tries to Ease Cyber Surveillance Fears," Reuters, October 16, 2014, https://www.reuters.com/article/southkorea-cybersecurity/south-korea-tries-to-ease-cyber-surveillance-fears-idUKL3N0SB1BH20141016; Song Ho-kyun and Jung Hwan-bong, "More and More S. Koreans Going Into 'Cyber Exile,'" *Hankyoreh*, October 7, 2014, http://english.hani.co.kr/arti/english_edition/e_national/658702.html; "Cyber Exodus, *Korea Herald*, October 6, 2014, http://m.koreaherald.com/view.php?ud=20141006000376&np=169&mp=17; and Kim Hyo-jin, "Somebody May Be Watching," *Korea Times*, January 1, 2015, https://m.koreatimes.co.kr/pages/article.amp.asp?newsIdx=170941.

381 Korean Legislation Research Institute's Korea Law Translation Center, "Telecommunications Business Act." See Enforcement Decree and Article 30.

382 Korean Legislation Research Institute's Korea Law Translation Center, "Telecommunications Business Act." See Article 22, Paragraph 1.

383 Korean Legislation Research Institute's Korea Law Translation Center, "Telecommunications Business Act." See Article 27.

384 Korean Legislation Research Institute's Korea Law Translation Center, "Telecommunications Business Act." See Article 92, Paragraph 1; and Korean Legislation Research Institute's Korea Law Translation Center, "Act on Promotion of Information and Communications Network Utilization and Information Protection," Korean Legislation Research Institute's Korea Law Translation Center, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=55570&lang=ENG. See Article 64, Paragraph 4. Also see Korean Legislation Research Institute's Korea Law Translation Center, "Telecommunications Business Act." See Article 92, Paragraph 1.

385 Kelly Kim, "The Court Held the System Unconstitutional for 'Infringement on the Freedom of Anonymous Expression' in the Constitutional Complaint Filed by Open Net," Open Net Korea, February 1, 2021, http://opennetkorea.org/en/wp/3179.

386 Korean Legislation Research Institute's Korea Law Translation Center, "Telecommunications Business Act." See Article 32-4, Paragraph 2; Korean Legislation Research Institute's Korea Law Translation Center, "Game Industry Promotion Act," Korean Legislation Research Institute's Korea Law Translation Center, https://elaw.klri.re.kr/eng_mobile/

viewer.do?hseq=46844&type=part&key=17. See Article 12-3, Paragraph 1, Item 1; and Korean Legislation Research Institute's Korea Law Translation Center, "Act on Promotion of Information and Communications Network Utilization and Information Protection." See Article 44-5.

387 Korean Legislation Research Institute's Korea Law Translation Center, "Act on Promotion of Information and Communications Network Utilization and Information Protection." See Article 23-3. See also Jihwan Park, "Stop Telecoms From Collecting Resident Registration Numbers! Abolish the 'Designated' Identity Verification Agencies!," Open Net Korea, March 7, 2014, http://opennetkorea.org/en/wp/836. For more information, see Jang Gyehyun and Lim Jong-In "Technologies of Trust: Online Authentication and Data Access Control in Korea," Carnegie Endowment for International Peace, August 17, 2021, https://carnegieendowment.org/2021/08/17/technologies-of-trust-online-authentication-and-data-access-control-in-korea-pub-85163.

388 Korean Legislation Research Institute's Korea Law Translation Center, "Act on Promotion of Information and Communications Network Utilization and Information Protection." See Article 44-2. Also see Kyung Sin "KS" Park, "From Liability Trap to the World's Safest Harbour: Lessons from China, India, Japan, South Korea, Indonesia, and Malaysia," *Oxford Handbook of Online Intermediary Liability*, August 2020, https://www.researchgate.net/publication/346718575_From_Liability_Trap_to_the_World's_Safest_Harbour_Lessons_from_China_India_Japan_South_Korea_Indonesia_and_Malaysia_published_in_Oxford_Handbook_of_Online_Intermediary_Liability.

389 Korean Supreme Court, "Compensation (Miscellaneous), etc.," Korean Supreme Court, Judgment, 2009 Da 53812, April 16, 2008, https://www.law.go.kr/%ED%8C%90%EB%A1%80/(2008%EB%8B%A453812).

390 Korean Legislation Research Institute's Korea Law Translation Center, "Act on the Establishment and Operation of Korea Communications Commission," Korean Legislation Research Institute's Korea Law Translation Center, https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=33740&type=part&key=17. See Article 21, Item 4.

391 Kyung Sin "KS" Park, "Administrative Internet Censorship by Korea Communication Standards Commission," *Soongsil Law Review* 33 (January 2015): 91–115, https://ssrn.com/abstract=2748307; and "S. Korea Censored Over 200,000 Pieces of Online Data Last Year: Report," Yonhap News Agency, September 25, 2020, https://en.yna.co.kr/view/AEN20200925006000320.

392 Korean Legislation Research Institute's Korea Law Translation Center, "Youth Protection Act," Korean Legislation Research Institute's Korea Law Translation Center, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=38401&lang=ENG. See Article 26. (This law has since been abolished.)

393 Korean Legislation Research Institute's Korea Law Translation Center, "Game Industry Promotion Act." See Article 12-3, Paragraph 1, Item 3.

394 Korean Legislation Research Institute's Korea Law Translation Center, "Telecommunications Business Act." See Article 22-5.

395 Jimin Goo, "Is the Group Chat Video Also a Temple? . . . Examining the Censorship Controversy Over the 'Nth Method,'" *Dong-a Ilbo*, December 14, 2021, https://www.donga.com/news/Economy/article/all/20211214/110769891/1.

396 Telegeography, "Transit Price Research Report in Major Cities Around the World," Korea Internet Companies Association, November 2021, http://www.kinternet.org/policy/data/view/63.

397 Michael R. Nelson and Kyung Sin "KS" Park, "Afterword: Korea's Challenge to the Standard Internet Interconnection Model," Carnegie Endowment for International Peace, August 17, 2021, https://carnegieendowment.org/2021/08/17/afterword-korea-s-challenge-to-standard-internet-interconnection-model-pub-85166.

398 Business Korea, "Government to Ease Internet Regulations to Prevent Reverse Discrimination Against Local Firms," Business Korea, January 1, 2014 , http://www.businesskorea.co.kr/news/articleView.html?idxno=2324; and Business Korea, "Korean Gov't Plans to Address Reverse Discrimination in Using Internet Network," Business Korea, November 11, 2017, http://www.businesskorea.co.kr/news/articleView.html?idxno=19685.

399 Lim Young-shin, Hwang Soon-min, and Cho Jeehyun, "Naver, Kakao Chiefs Call for Actions to Address Reverse Discrimination Vs. Foreign Players," *Pulse News, October 22, 2021,* https://pulsenews.co.kr/view.php?sc=30800028&year=2021&no=1002282; and "KCC to Require Foreign Internet Companies to Follow Domestic Regulations," *Hankyoreh, December 13, 2018,* https://www.hani.co.kr/arti/english_edition/e_business/874295.html.

400 General Agreement on Tariffs and Trade, "Services Sectoral Classification List," General Agreement on Tariffs and Trade, MTN.GNS/W/120, July 10, 1991, https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=179576&CurrentCatalogueIdInd%20ex=0&FullTextHash=&HasEnglishRecord=True&HasFrenchRecord=True&HasSpanishRecord=True. Value-added services means, according to W/120, electronic mail, voicemail, online information and database retrieval, electronic data interchange, enhanced facsimile services, code and protocol conversion, and online information and/or data processing services. Meanwhile, computer and related services consist of, according to W/120, consultancy services, software implementation services, data processing services, database services, and others.

401 World Trade Organization Appellate Body Report, "United States-Measures Affecting the Cross-border Supply of Gambling and Betting Services," *("US—Gambling"),* ¶¶ 227-33, WTO Doc. WT/DS285/AB/R, March 23, 2005, https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm.

402 World Trade Organization Appellate Body Report, "China–Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products," ("China–Publications and Audiovisual Products"), ¶ 412, WTO Doc. WT/DS363/AB/R, January 19, 2010, https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds363_e.htm.

403 World Trade Organization, "General Agreement on Trade in Services," World Trade Organization, April 15, 1994, https://www.wto.org/english/tratop_e/serv_e/gatsintr_e.htm. See Article XVI on market access: "In sectors where market-access commitments are undertaken, the measures which a Member shall not maintain or adopt either on the basis of a regional subdivision or on the basis of its entire territory, unless otherwise specified in its Schedule, are defined as: (a) limitations on the number of service suppliers whether in the form of numerical quotas, monopolies, exclusive service suppliers or the requirements of an economic needs test; (b) limitations on the total value of service transactions or assets in the form of numerical quotas or the requirement of an economic needs test; (c) limitations on the total number of service operations or on the total quantity of service output expressed in terms of designated numerical units in the form of quotas or the requirement of an economic needs test; (d) limitations on the total number of natural persons that may be employed in a particular service sector or that a service supplier may employ and who are necessary for, and directly related to, the supply of a specific service in the form of numerical quotas or the requirement of an economic needs test; (e) measures which restrict or require specific types of legal entity or joint venture through which a service supplier may supply a service; and (f) limitations on the participation of foreign capital in terms of maximum percentage limit on foreign shareholding or the total value of individual or aggregate foreign investment."

404 World Trade Organization Appellate Body Report, "US—Gambling." Also see Markus Krajewski, National Regulation and Trade Liberalization in Services: The Legal Impact of the General Agreement on Trade in Services (GATS) on National Regulatory Autonomy," (Amsterdam: Kluwer Law International, 2003), 86, https://www.google.com/books/edition/National_Regulation_and_Trade_Liberaliza/K0RllJToadcC?hl=en&gbpv=1&dq=MARKUS+KRAJEWSKI,+NATIONAL+REGULATION+AND+TRADE+LIBERALIZATION+IN+SERVICES-+THE+LEGAL+IMPACT+OF+THE+GENERAL+AGREEMENT+ON+TRADE+IN+SERVICES+(GATS)+ON+NATIONAL+REGULATORY+AUTONOMY+86&pg=PT172&printsec=frontcover.

405 The two other available modes are consumption abroad and natural persons. For instance, in the U.S.-Korea Free Trade Agreement, the mode of commercial presence belongs to the investment chapter while the three other modes belong to the cross-border trade chapter. Relevantly, this trade agreement prohibits state parties from requiring service providers to shift into the commercial presence mode. Article 12.5 states, "Neither Party may require a service supplier of the other Party to establish or maintain a representative office or any form of enterprise, or to be resident, in its territory as a condition for the cross-border supply of a service." See Office of the U.S. Trade Representative, "U.S.-Korea Free Trade Agreement: Final Text (as of January 1, 2019," Office of the U.S. Trade Representative, January 1, 2019, https://ustr.gov/trade-agreements/free-trade-agreements/korus-fta/final-text.

406 World Trade Organization Panel Report, "China—Certain Measures Affecting Electronic Payment Services," ("China—Electronic Payment Services"), ¶ 7.687, WTO Doc. WT/DS413/R and Add.1, August 31, 2012, https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds413_e.htm; and World Trade Organization Appellate Body Report, "Argentina—Measures Relating to Trade in Goods and Services" ("Argentina—Financial Services"), ¶ 6.34, WTO Doc. WT/DS453/AB/R, April 14, 2016, https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds453_e.htm.

407 World Trade Organization Appellate Body Report, "European Communities—Regime for the Importation, Sale and Distribution of Bananas" ("EC—Bananas III"), ¶ 241, WTO Doc. WT/DS27/AB/R, September 25, 1997, https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds27_e.htm; and World Trade Organization Appellate Body Report, *"Argentina—Financial Services",* ¶ 6.106.

408 World Trade Organization Appellate Body Report, "US—Gambling," ¶ 3.150.

409 Ibid. ¶ 6.287.

410 World Trade Organization Panel Report, "Canada—Certain Measures Affecting the Automotive Industry" ("Canada—Autos,") ¶ 10.307, WTO Doc. WT/DS139/R, WT/DS142/R, February 11, 2000, https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds139_e.htm.

411 World Trade Organization, "General Agreement on Trade in Services"; and World Trade Organization, "Marrakesh Agreement Establishing the World Trade Organization," Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167, 1994, https://www.wto.org/english/docs_e/legal_e/04-wto_e.htm.

412 World Trade Organization, "WTO Analytical Index: GATS – Article XIV (Jurisprudence)," World Trade Organization, https://www.wto.org/english/res_e/publications_e/ai17_e/gats_art14_jur.pdf. Also see World Trade Organization Appellate Body Report, "US—Gambling," Paragraph 339.

413 Sacha Wunsch-Vincent, "The Internet, Cross-Border Trade in Services, and the GATS: Lessons from US—Gambling," *World Trade Review* 5 (2006): *319, 320–322,* https://www.piie.com/commentary/speeches-papers/internet-cross-border-trade-services-and-gats-lessons-us-gambling.

414 Rolf H. Weber and Rainer Baisch, "Revisiting the Public Moral/Order and the Security Exceptions Under the GATS," *Asian Journal of WTO and International Health Law and Policy* 13, no. 2 (2018), 375, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3256716.

415 U.S. International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 1, U.S. International Trade Commission Publication* 4415, (Washington, DC: U.S. International Trade Commission, 2013*),* https://www.usitc.gov/publications/332/pub4415.pdf; and Rachel F. Fefer, Shayerah I. Akhtar, and Michael D. Sutherland, "Digital Trade and U.S. Trade Policy," Congressional Research Service, December 9, 2021, https://fas.org/sgp/crs/misc/R44565.pdf.

416 European Commission, "Report From the Commission to the European Council: Trade and Investment Barriers Report 2015," European Commission, March 17, 2015, http://trade.ec.europa.eu/doclib/docs/2015/march/tradoc_153259.pdf.

417 European Commission, "Horizontal Provisions for Cross-Border Data Dlows and for Personal Data Protection (in US Trade and Investment Agreements," in *EU Trade and Investment Agreements*, May 2018, https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf.

418 Office of the U.S. Trade Representative, "The Trans-Pacific Partnership: Promoting Digital Trade," Office of the U.S. Trade Representative, 2015, https://ustr.gov/sites/default/files/TPP-Promoting-Digital-Trade-Fact-Sheet.pdf.

419 Jonah Force Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," Lawfare Research Paper Series 2, no. 3 (July 21, 2014), https://s3.documentcloud.org/documents/7276302/THE-GROWTH-OF-DATA-LOCALIZATION-POST-SNOWDEN.pdf.

420 Susan Ariel Aaronson, "Data Is Different: Why the World Needs a New Approach to Governing Cross-Border Data Flows," Centre for International Governance Innovation Paper No. 197, November 14, 2018, https://www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows.

421 Susan Aaronson, "Why Trade Agreements Are Not Setting Information Free: The Lost History and Reinvigorated Debate Over Cross-Border Data Flows, Human Rights, and National Security," *World Trade Review* 14, no. 4 (October 2015): 671–700, https://elliott.gwu.edu/sites/g/files/zaxdzs2141/f/Aaronson%20World%20Trade%20Review%202015.pdf.

422 Aaronson, "Why Trade Agreements Are Not Setting Information Free," 19.

423 Sarah Box, "Internet Openness and Fragmentation: Toward Measuring the Economic Effects," Global Commission on Internet Governance (Center for International Governance Innovation and Chatham House), Paper Series No. 36, 2016, https://www.cigionline.org/sites/default/files/gcig_no.36_web.pdf; and Sarah Box and Jeremy K. West, "Economic and Social Benefits of Internet Openness," *Organisation for Economic Co-operation and Development (OECD), OECD Digital Economy Series No. 257, 2016,* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2800227.

424 U.S. Department of State, "The Clean Network," U.S. Department of State, 2021, https://2017-2021.state.gov/the-clean-network/index.html.

425 Aaronson, "Data Is Different: Why the World Needs a New Approach to Governing Cross-Border Data Flows."

426 U.S. Department of State, "Declaration for the Future of the Internet," U.S. Department of State, https://www.state.gov/declaration-for-the-future-of-the-internet.

427 Aaronson, "Why Trade Agreements Are Not Setting Information Free."

428 Kelly Kim, "Open Net Filed a Lawsuit Against KCSC to Restore a P2P 4shared.com," Open Net Korea, March 11, 2015, http://opennetkorea.org/en/wp/1313.

429 Kate Jee-hyung Kim, "Lessons Learned From South Korea's Real-Name Policy," *Korea Industry and Technology Times*, January 15, 2012, http://www.koreaittimes.com/news/articleView.html?idxno=19361.

Carnegie Endowment for International Peace

The Carnegie Endowment for International Peace is a unique global network of policy research centers in Russia, China, Europe, the Middle East, India, and the United States. Our mission, dating back more than a century, is to advance peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decisionmakers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

Asia Program

In Asia, rapid growth and strong economic fundamentals have lifted hundreds of millions from poverty. But significant cracks have emerged in this hopeful story. The Carnegie Asia Program explores three disruptive risks to Asia's future: (1) disruptive security risks, from competition among the big powers; (2) disruptive governance risks, from uneven state capacity or insufficiently inclusive growth; and (3) disruptive technological risks, arising from new innovations, regulatory diversity, or competing standards. Our program recommends policies to manage the growing threats to Asia's long peace. We also help decisionmakers address social, institutional, and political obstacles to achieving Asia's development potential.

Technology and International Affairs Program

The Carnegie Technology and International Affairs Program develops strategies to maximize the positive potential of emerging technologies while reducing risk of large-scale misuse or harm. With Carnegie's global centers and an office in Silicon Valley, the program collaborates with technologists, corporate leaders, government officials, and scholars globally to understand and prepare for the implications of advances in cyberspace, biotechnology, and artificial intelligence.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org