ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Friday, March 8, 2019

Mr. Goonjan Kumar
Assistant Director
Department for Promotion of Industry and Internal Trade
India's Ministry of Commerce and Industry
Udyog Bhawan,
New Delhi, 110011, India

RE: Draft National E-Commerce Policy

Dear Mr. Kumar:

I write in response to the Department for Promotion of Industry and Internal Trade's request for comments from stakeholders on India's draft national e-commerce policy.

The Information Technology and Innovation Foundation (ITIF) is a non-profit, non-partisan research and educational institute—a think tank—whose mission is to formulate, evaluate, and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress. ITIF's goal is to provide policymakers around the world with high-quality information, analysis, and recommendations they can trust. On the strength and influence of this work, the University of Pennsylvania has ranked ITIF as the world's leading think tank for science and technology policy, and one of the top 50 U.S. think tanks of any type.

ITIF's submission draws on an extensive body of our work on many issues raised in the draft national e-commerce policy, including data-driven innovation, data privacy and protection, regulatory access to data, the Internet of Things (IoT), intellectual property, data and anti-trust, and other policies related to e-commerce and the global digital economy. Reports from ITIF and its Center for Data Innovation include: "Data Innovation 101: An Introduction to the Technologies and Policies Supporting Data-Driven Innovation," "10 Policy Principles for Unlocking the Potential of the Internet of Things," "The State of Data Innovation in the EU," "Cross-Border Data Flows Enable Growth in All Industries," "The Indian Economy at a Crossroads," and "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?"

I—Nigel Cory—make this submission on behalf of ITIF.

Sincerely,

Nigel Cory
Associate Director, Trade Policy, The Information Technology and Innovation Foundation

CONTENTS

Introduction 2
Creating a Policy Framework for a Data-Driven Economy 6
Key Policies and Principles to Support Data-Driven Innovation 6
Principles for Unlocking the Potential of the Internet of Things 8
Getting Data Governance Right on Privacy, Cybersecurity, and Regulatory Access to Data 10
Data Privacy and Protection—The Misguided Focus on the Geography of Data Storage 11
Regulatory Oversight and Focusing on Access to Data (Not Where Data is Stored) 13
Digital Customs Duties—Avoid Raising Costs and Breaking a Global Consensus 15
Data and Competition Policy—Focus on Anti-Competitive Behavior, Not the Amount of Data 16
The Impact and Cost of Digital Protectionism and Innovation Mercantilism 17
Research Shows that Barriers to Data Flows Undermine Firm Competitiveness and Economic Productivity 19
E-Commerce, Small Package Trade, and Trade Facilitation 20
E-Commerce, Intellectual Property, and Voluntary Agreements 22
Example: The United States: Domain Name Registries—Trusted Notifier Programs 24
Example: Infringing Website Lists and "Follow the Money" Efforts to Target Piracy Profits ... 25
Intellectual Property and Source Code—Forced Disclosure as a Barrier to Trade and Innovation 26
Conclusion 28
Annex 29
Endnotes 31

INTRODUCTION

India's draft National E-Commerce Policy (the "Policy") rightly recognizes many policy issues, concepts, and technologies that will determine the success of its digital economy, especially the role of data (see the annex for a summary of the draft Policy's key goals).[1] India should be commended for taking such a holistic view of the policy framework. However, the draft Policy includes a range of misguided and harmful policy proposals that together reflect a short-term, mercantilist approach to digital development. Most importantly, a misguided focus on the control and location of data in India will reduce the potential social and economic utility of data. Similarly, an overriding focus on supporting local tech firms and facilities (essentially import substitution but for domestic data processing and computing facilities) and prioritizing exports over imports is missing the point as to the broader economic benefits of digital technologies. Just as economic nationalism inevitably leads to lower productivity for firms and higher costs for consumers, "data nationalism" will similarly lead to poor economic outcomes as these policies will detract from India's ability to benefit from data-driven innovation, increase the cost of key capital goods, likely lead to broad economic inefficiencies, and harm India's globally competitive information technology (IT) sector, among other ramifications.[2] This

submission highlights some of the draft Policy's positive proposals and analyzes why many other provisions are misguided or mistaken (while proposing alternative policies in some areas).

The draft Policy rightly focuses on data as it, along with information communication technologies (ICTs), will play an increasingly important role in supporting economic productivity and innovation. The increased digitalization of organizations, driven by the rapid adoption of technologies such as cloud computing and data analytics, has increased the importance of data as an input to commerce, impacting not just information industries, but traditional industries as well. In terms of a quantitative analysis of the economic impact of cross-border data flows, it has been estimated that globally 75 percent of the value added by the Internet and data flows occurs in traditional industries, in part through increases in productivity.[3] The use of data analytics in virtually all industries has streamlined business practices and increased efficiency, but also made the movement of data more important.[4] Organizations increasingly rely on data for a number of purposes, including to monitor production systems, manage global workforces, monitor supply chains, and support products in the field in real time. Companies collect and analyze personal data to better understand customers' preferences and their willingness to pay, and adapt their products and services accordingly. It is a simple fact that international trade involving consumers cannot take place without collecting and sending personal data across borders—data such as names, addresses, billing information, etc.[5]

Indeed, data is the lifeblood of the modern global economy. Data-driven innovation is making a significant mark around the world because the rapid growth in the ability to collect, store, analyze, and share large quantities of information at low cost drives new forms of economic activity, scientific discovery, and social innovation. Digital trade and cross-border data flows are expected to continue to grow faster than the overall rate of global trade. Globally, McKinsey analysis finds that, over the past decade, data flows have increased world GDP by 10.1 percent.[6]

India has already been a major beneficiary of digital technologies and the ability for data to flow freely across borders. With the liberalization of the Indian economy, the Information Technology and Business Process Management (ITBPM) sector has seen exponential growth—from a mere 1.2 percent of Indian GDP in 1998 to 9.5 percent in 2015.[7] India is the world's leading provider of IT-based business services, accounting for approximately 55 per cent of the US$185-190 billion global services outsourcing business in 2017-18.[8] India's IT and IT-enabled services industry grew to US$167 billion in 2017-18. Exports from India's IT industry increased to US$126 billion in FY18. The computer software and hardware sector in India attracted foreign direct investment (FDI) inflows worth US$32.23 billion between April 2000 to June 2018.[9] India's leading role in IT services exports (i.e., services trade that depends on data flows) has had a spillover effect, including in developing strong IT-capable human resources. Indian policymakers need to keep this sector in mind, as many of the provisions in the draft Policy would put this sector's success at risk.

India should reconsider many of the draft Policy's proposals as a globally competitive and innovative digital economy in India will in part depend on the ability of individuals and firms to engage in commerce without unnecessary and discriminatory restrictions, and geographic barriers, on how firms can use and transfer data.[10] Indian policymakers should take a careful, considered approach as the Indian government considers enacting key policies that relate to data, such as for data privacy and protection, regulatory access to data, anti-trust, and intellectual property. Beyond the draft Policy, policymakers in India are currently considering how to

enact key laws and regulations that will have a major impact on India's digital economy. Many of this submission's recommendations also apply to these other draft laws and regulations. The following sections provide a detailed analysis of some of the key provisions in the draft policy.

However, underpinning all of ITIF's analysis and recommendations are some fundamental principles that policymakers should keep in mind as they consider policy changes:

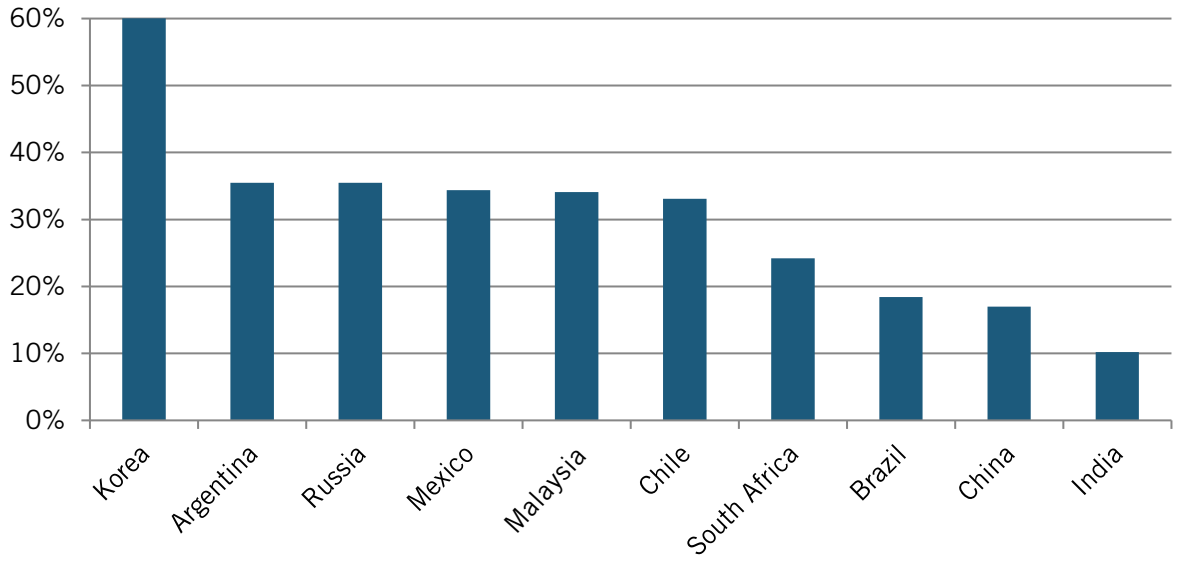
Reduce or eliminate artificial costs for ICT products and digital goods and services. As ITIF outlines in "A Policymaker's Guide to Spurring ICT Adoption," cost is a major driver of adoption for consumers and firms alike, as rising prices generally lead to falling demand.[11] This should be a central concern as the cost of Internet access remains beyond the reach of many millions of Indians. ICTs are particular important to focus on as they represent a key "general purpose technology" which supports economic productivity.[12] In a conclusive review of over 50 scholarly studies on ICT and productivity published between 1987 and 2002, Dedrick, Gurbaxani, and Kraemer found that "the productivity paradox as first formulated has been effectively refuted. At both the firm and the country level, greater investment in ICT is associated with greater productivity growth."[13] In fact, nearly all scholarly studies from the mid-1990s have found positive and significant effects of ICT on productivity.[14] The beneficial effects of ICT on productivity have been found across different levels and sectors of economies, from firms to industries to entire economies, and in both goods- and services-producing industries.[15]

This means policymakers should aim to eliminate (and avoid introducing further) tariffs and discriminatory taxes and ensure that users can buy best-in-class technology from anywhere in the world (e.g., remove local content requirements, limits on foreign direct investment, and restrictive certification or licensing arrangements). For example, Kaushik and Singh found that for every $1 of tariffs India imposed on imported ICT products, India suffered an economic loss of $1.30 because of lower productivity.[16] India has the potential to reduce the prices for many goods given its existing use of tariffs and other measures that increase cost, as shown in ITIF's report "Digital Drag: Ranking 125 Nations by Taxes and Tariffs on ICT Goods and Services."[17] For example, in India's 2014 budget, India announced new 10 percent tariffs on ICT and other goods in its July 2014 budget, even though it is currently a member of the Information Technology Agreement.[18] Tariffs on capital goods such as ICTs only stifle adoption and deployment of these innovation- and productivity-enhancing tools, which slows broader Indian economic growth.

India's greatest economic challenge is bolstering its productivity.[19] As Figure 1 shows, the level of Indian labor productivity trails that of other developing countries such as Argentina, Russia, Mexico, Malaysia, Brazil, and China. And even though labor productivity levels in Brazil and China are still less than 20 percent of U.S. levels, their productivity levels (as a percentage of the U.S. level) are still more than 70 percent higher than India's Moreover, India's productivity gap compared to peer developing nations has generally grown over the past four decades. For example, China started off with one-third of India's productivity level in 1970; four decades later Chinese productivity level is 67 percent higher.[20] In fact, growth in Chinese labor productivity has significantly outstripped India's since the year 2000.[21] Emphasizing this point, the Asian Productivity Organization's *2012 Productivity Databook* noted that, in part because of the disparity in their sectoral productivity levels, "all sectors of China's economy grew faster from 2000 to 2009 than those of India, except for transport, storage, and communications, showing India's special strength in ICT services."[22] India's draft

Policy should emphasize how Indian policymakers can assist Indian businesses, especially small firms, in leveraging digital tools to bolster their productivity across every sector of the economy.

Figure 1: Select Country Labor Productivity as Percent U.S. Level, 2012.[23]



The value of data comes from the insights that individuals and firms are able to derive from it, not from the data center or country the data is stored in. Recent technological advancements—such as faster computing, better algorithms, and more-robust communication networks—have made it easier and cheaper to collect, store, analyze, use, and disseminate data. The draft Policy recognizes the central role that data plays in the modern economy; however, it misdirects much of its policy attention in the misguided direction that the location of data matters in maximizing the value of data. It doesn't. Success in the data economy depends on how effectively firms can leverage data to generate insights and unlock value. For many firms, major gains will come from getting as many firms as possible to adopt and use off-the-shelf computer software and cloud services to help them better collect, access, and analyze their own data or that from third-party services and to use cloud-based analytics platforms to provide insights from the data. For others, the challenge is developing and deploying artificial intelligence and machine learning tools for their own operations and as third-party consultants to others. Enacting artificial barriers to data flows and forcing firms to store data in local data centers does not improve data-driven innovation. The leverage India gets from trying to exert control over where data is stored or processed is exceedingly low; Indian policymakers would generate far more benefit from assisting Indian firms in understanding how they can create value through data analytics or by creating data streams around manufactured or agricultural goods.

Responsibility should flow with data. Policymakers should put responsibility at the heart of their policy framework for data privacy, protection, and regulatory oversight. The firm that collects the data is legal responsibility for abiding by data-related laws, wherever the data is stored. And firms are responsible for how their third-party business partners, affiliates, etc. use their consumers' data. If a firm operates within a country's jurisdiction, by providing goods or services to customers in a country, it has "legal nexus" in the

country and thereby has to follow that country's laws. Countries should focus on holding firms accountable for how they manage data, not on where it is stored. A company can't escape Indian laws by simply transferring data out of the country—the responsibilities accompany the data. This focus on responsibility also reflects the critical fact that modern technology, especially globally distributed technologies like the Internet and cloud data storage, means that each country's domestic regulatory regime for data, such as privacy, needs to be global in scope and application. The international extension of this policy focus is that each country's regulatory regime needs to be interoperable, as each country faces the same challenges in applying their laws to firms that may transfer data between jurisdictions.

CREATING A POLICY FRAMEWORK FOR A DATA-DRIVEN ECONOMY

Creating more-restrictive data privacy or regulatory laws is rather straightforward, but creating such laws to have minimal disruptive effects on users and businesses is much more complex, which is why India should include innovation as an explicit outcome in relevant laws and regulations, and ensure innovation is considered when carefully reevaluating each proposed provision. The following section outlines some problematic provisions in the draft Policy and provides some alternative suggestions for Indian policymakers in considering how best to support e-commerce and data-driven innovation.

Key Policies and Principles to Support Data-Driven Innovation

Data innovation—the innovative use of data to create social and economic benefits—is critically important to firm and economic competitiveness. In business, an array of data-driven tools can help companies streamline their business processes and become more responsive to their customers.[24] The draft Policy rightly recognizes the importance of data-driven innovation in making the overarching point that (page 11) "creating economic benefits from data, that is, monetization of data, is an important business model adopted by many corporations to generate profits by analyzing, processing and utilizing data" and that "access to data can lead to the development of a large number of innovative solutions." However, many of the Policy's recommendations are mistaken in how they envision India and Indian firms and users can access and benefit from data.

India's draft Policy includes a number of misconceptions (see the annex) about data, data-driven innovation, data-intensive firms, and e-commerce (some of which will be explored in greater detail later in the submission). Firstly, as highlighted above, the value of data comes from the insights firms and individuals are able to derive from it, not from the location of its storage. This misconception is best encapsulated in the following section from the draft Policy (page 15): "At this juncture there is no legal framework that would permit the government to impose restrictions on cross-border flow of data. Without having access to the huge trove of data that would be generated within India, the possibility of Indian business entities creating high value digital products would be almost nil. Domestic technology companies would be merely processing outsourced data work. Further, by not imposing restrictions on cross-border data flow, India would itself be shutting the doors for creation of high-value digital products in the country." Conceptually, data flows and digital products and services should be able to flow (nearly) seamlessly across borders to firms and consumers situated throughout the world. Businesses use data to create value, and many can only maximize that value when data can flow freely across borders. The success of India's IT sector is a testament to this fact. However, the draft Policy fails to recognize this central point.

Secondly, the use of data is non-rivalrous, meaning that one person's or enterprise's use of it does not diminish its availability to other users. For example, the value to one advertising network of knowing a user's age and location is not affected by whether another advertising network also has that information. Thirdly, data-driven companies benefit from network and scale effects, but this is not undesirable in-and-of itself, as these deliver significant benefits to society.[25] Data-intensive firms face fierce competition and low entry barriers in many of their most lucrative markets, so these concepts, along with an almost zero marginal cost of production for information industries, means that market conditions constantly change. Examples of firms that saw their dominance eroded abound. MySpace and Friendster lost to Facebook; AltaVista and Lycos lost to Google; Blackberry and Nokia were displaced by the iPhone, which now competes against Android phones.

India should instead focus on three key issues in examining how to use policy to support data-driven innovation (as drawn from ITIF's Center for Data Innovation's report "The State of Data Innovation in the EU").[26]

- **Maximize the supply of reusable data.** Governments should both avoid laws and regulations that stifle the supply and flow of data, such as overly burdensome data-protection rules and data-localization policies in different member states, and increase the supply of data, such as via open data and freedom-of-information policies.[27] India should avoid enacting barriers to cross-border data flows and excessive restrictions that limit the benefits of data-driven innovation, such as restrictive privacy rules. Such limitations are not only unnecessary, but dangerous, because they inhibit innovations that could protect and improve people's lives.[28] Given that these data-related issues cut across many different agencies, India should also ensure that it does not create regulatory fragmentation by allowing different agencies and laws to create their own restrictive data-related regulations or overlapping and contradictory data-related rules and regulations, as this would undermine the supply and ability for data to flow within India and between India and the rest of the world.[29]
- **Improve infrastructure that supports data innovation.** The draft Policy is right to recognize infrastructure as a priority issue for e-commerce. Internet penetration in India has improved considerably in recent years, but still has considerable progress to go. Internet penetration in urban India was 64.8 percent in December 2017 as compared to 60.6 percent last December. In comparison, rural Internet penetration increased from 18 percent in December 2016 to 20.2 percent in December 2017.[30] India's national, state, and city governments should encourage the development and deployment of key technological platforms that enable data innovation, such as broadband, digital public services, smart meters, and smart cities. India's inadequate fiber-optic network leads to poor-quality data services and inconsistency of coverage, holding back the spread of the mobile Internet in semi-urban and rural parts of the country. Where the market fails to serve sparsely populated areas adequately, governments should step in with direct investment and leadership in public-private partnerships. India is already taking steps in the right direction through its smart cities mission and in establishing the Bharat Broadband Network to extend fiber-optic cable to 250,000 villages.[31]

- **Develop data-science and data-literacy skills in workers.** India should encourage the development of data-related skills through its education system and through professional training programs. Similar to many other countries, India has a lot of work to do here. According to a survey by market research firm IMRB, while 48 percent of urban Indians are computer literate, just 14 percent of rural Indians are.[32] A recent report by knowledge portal Analytics Vidhya and ed-tech platform Great Learnings showed that more than 50,000 positions related to data and analytics were vacant in India.[33] However, the scarcity of data analytics talent is particularly acute in India given its role as a hub for outsourced technology services work, with global companies sending an increasing number of data-related work to the country. The demand for data-science and data-literate workers will only increase. Indian IT industry estimate show that firms could hire up to three million more workers by 2025.[34]

Principles for Unlocking the Potential of the Internet of Things

The draft Policy's focus on the Internet of Things is pertinent given the role it will play in the country's digital economy.[35] The Internet of Things encapsulates the idea that ordinary objects—from thermostats and shoes to cars and lamp posts—will be embedded with sensors and connected wirelessly to the Internet. These devices will then send and receive data which can be analyzed and acted upon. As the technology becomes cheaper and more robust, an increasing number of devices will join the Internet of Things. Though many of the changes to everyday devices may be subtle and go unnoticed by consumers, the long-term effect could ultimately have an enormously positive impact on individuals and society. A connected world is capable of anything from improving personal health to reducing pollution to making industry more productive. The Internet of Things offers solutions to major social problems, but this vision of a fully connected world will not be achieved without initiative and leadership from policymakers to promote its deployment and avoid pitfalls along the way.

However, the draft Policy includes a range of measures which would undermine the development, deployment, and adoption of the Internet of Things and the data that these connected devices will generate:

- **Page 16**—"A legal and technological framework to be created that can provide the basis for imposing restrictions on cross-border data flow from the following specified sources: a) Data collected by IoT devices installed in public space b) Data generated by users in India by various sources, including ecommerce platforms, social media, search engines etc. The legal and technological framework would also provide basis for sharing the data collected by IoT devices under (a) above with domestic entities for use in research and development for public policy purposes."

- **Page 30**—"Domestic industrial standards need to be formulated and facilitated for smart devices and IoT devices to meet the goals of the country including, inter alia, consumer protection, secured transactions, enhanced interoperability and ease-of-user interface. National standard-setting organizations will be involved in this exercise along with other stakeholders."

As to the first point, as explained in this submission, India should not impose restrictions on cross-border data flows for data collected by Internet of Things devices installed in public spaces and solely allow domestic firms to access and use this data for research purposes. The value of data comes from the insights firms are able to derive from it, and for firms to maximize the potential value of data, it needs to flow. Enacting artificial barriers on the flow of data and which parties can access and use it limits the potential value of the data as it may prevent the best-placed firms from analyzing it. Moreover, as noted above, in most instances data localization mandates do not increase commercial privacy nor data security.[36]

As to the second point, India should avoid developing India-specific standards for Internet of Things devices. One reason why the Internet economy has flourished world-wide is because industry collaborated to develop interoperable global standards. This is why a traveler from India to any other nation can be assured that their cell phone, web browser, laptop and thumb drives will all work. The last thing nations need to do is to develop nation-specific Internet standards. Developing nation-based ICT standards also raise significant barriers to ICT competitiveness, as ITIF documented in its report "The Middle Kingdom Galapagos Island Syndrome: The Cul-De-Sac of Chinese Technology Standards," because while indigenous standards may seem like a good idea in the short run by boosting domestic market share held by local firms, they represent a fundamentally bad idea in the long run as they make it much harder for local firms to achieve the global scale so critical for success in ICT industries.[37] Instead, India should adopt international standards so as to promote interoperability between different countries' standards systems. Ensuring standards are compatible fosters economies of scale by making it relatively easy for firms to produce a good/service to a mutually accepted standard across markets. Technology companies need to be able to use interoperable standards across markets in order to help keep unit prices low, which supports deployment and adoption of ICTs.[38] Well-organized, open, and transparent standards systems promote compatibility of key components in national infrastructure—especially in high-tech sectors such as telecommunications and computer networks.[39] In essence, standards form a bridge between markets and technologies.

Instead of developing its own standards to attempt to gain competitive advantage, Indian policymakers should consider the Center of Data Innovation's report "10 Policy Principles for Unlocking the Potential of the Internet of Things" and its recommendations as a blueprint for India's approach to Internet of Things policies, which should have the overall aim to promote adoption, increase the value of data collected from connected devices, and maximize the benefits of the Internet of Things for consumers, government, and industry.[40] These policies reflect the status of the Internet of Things as an emerging technology that requires a policy framework that is fully cognizant of its benefits, allows for future innovation, and responsibly protects against misuse without restricting its capacity to deliver social, civic, and economic benefits.

The ten recommendations include:

1. **Chart the Course for Adoption:** Every nation should develop a strategic roadmap to guide the deployment and adoption of the Internet of Things.

2. **Lead by Example:** The government should be an early adopter of the Internet of Things to demonstrate the benefits of the technology.

3. **Look to Partnerships to Overcome Obstacles:** Many Internet of Things projects will benefit from government agencies establishing partnerships with both the private sector and others in government.

4. **Reduce Regulatory Barriers and Delays for Getting Smart Devices to Market:** A lengthy and cumbersome regulatory review process that increases the time to market for smart devices can discourage entrepreneurs from developing new and potentially life-saving products.

5. **Minimize the Regulatory Cost of Data Collection:** Policymakers should create laws and regulations that allow businesses and governments to build products and services efficiently, using the highest-quality, most-complete data possible.

6. **Make it Easy to Share and Reuse Data:** The Internet of Things will generate an unprecedented quantity of data, and policymakers should be careful not to equate simple data sharing with harmful misuse.

7. **Relentlessly Pursue Better Data:** With ever-higher-quality sensors and an increasing number of them, the Internet of Things allows for the capture of an unprecedented quantity and quality of data. Policymakers should continue to invest in opportunities to collect more granular, timely, and complete data.

8. **Reduce the "Data Divide":** Policymakers should encourage widespread adoption of connected devices, from wearable fitness trackers to sensors on street corners, to close the "data divide"—the social and economic inequalities that may result from a lack of collection and use of data about an individual or community.[41]

9. **Use Data to Tackle Hard Problems:** While the Internet of Things offers many economic benefits, policymakers need to ensure that opportunities to use these devices to address important social issues, such as health care and public safety, are also a top priority.

10. **Where Rules Are Needed to Protect Consumers, Keep Them Narrow and Targeted:** Many technologies are often met with fear, uncertainty, and doubt, especially by those who are unfamiliar with them or opposed to change. Policymakers cannot afford to succumb to these forces if they expect to enable society to take full advantage of the Internet of Things. In particular, policymakers should be extremely cautious about regulating on the basis of purely speculative concerns that might not even come to pass, especially when doing so might curtail substantial economic and social benefits, many of which are already being realized today.[42]

Getting Data Governance Right on Privacy, Cybersecurity, and Regulatory Access to Data

India's draft Policy rightly recognizes that e-commerce covers a wide range of public policy issues, including privacy, cybersecurity, and regulatory oversight.[43] The draft Policy specifically references privacy and data security in a number of provisions. While the draft Policy does not explicitly call for forced data localization as a privacy, cybersecurity, and regulatory measure, its call for data localization in order to support e-commerce more broadly likely means the authors are supportive of such requirements given recent India laws

or proposals to enact data localization. For example, India's draft privacy law requires data localization, while the Reserve Bank of India recently enacted data localization for payments data.[44] This widespread focus on the location of data storage in India is misguided. As previously mentioned, the value of data comes from the insights firms and individuals are able to derive from it, not the location where data is stored or processed. Furthermore, the sections below outline how policymakers are mistaken in thinking that local data storage improves data privacy and data protection or that forced local data storage is the best way to provide regulatory oversight.

As in this submission's guiding principles, the basic expectation policymakers should have is that when it comes to handling data, companies doing business in a country should be responsible for their own actions and the actions of both their agents and business partners, regardless of whether they're located outside the country where a firm collects and/or manages data. For example, this could be made clear in law by declaring that companies doing business in a country are legally responsible for any failures to protect the personal data of that country's citizens, regardless of whether those failures are the fault of the company in that country, or an affiliate or business partner in another nation. In other words, a country's data-related responsibilities would travel with the data, regardless of where the data travels. Companies doing business in a given country would then have a strong incentive to assist their business partners outside that country in adhering to its local laws (such as privacy), because its citizens and the government could seek remedies for any violations. This responsibilities-focused approach to data is the realistic alternative to the false (and economically damaging) notion that data must be stored domestically in order to ensure it remains secure and private.

Data Privacy and Protection—The Misguided Focus on the Geography of Data Storage

India should take a careful and considered approach to enacting its own data protection and privacy regimes. Privacy policy in India is in a state of flux with the report by the "committee of experts," the Supreme Court of India's ruling that the right to privacy is a fundament right, and the Supreme Court's ruling that established the individual's control over their data.[45] For example, as India considers its own data privacy framework, it would be well advised to avoid "copying and pasting" the European Union's approach to data privacy and protection and scrutinize each individual privacy provision, including data controller/processor registration, an "adequacy" approach to international data transfers, explicit consent, and the right-to-be-forgotten. India should do this because privacy rules represent key building-block laws that have a considerable impact on a country's digital economy and its ability to benefit from digital trade.

The draft Policy makes the false connection between the geography of data storage and processing and data protection by associating international transfers with risks and dangers. In the section on "not just a privacy issue," the Draft policy states that "At this juncture there is no legal framework that would permit the government to impose restrictions on cross-border flow of data."[46] The notion that data must be stored domestically in order to ensure it remains secure and private is false. Policymakers focusing on geography to solve cybersecurity and privacy concerns are missing the point. Consumers and business can rely on contracts or laws to limit voluntary disclosures to ensure data stored abroad receives the same level of protection as data stored at home. Controlling where organizations store data does not impact how organizations collect and use data (privacy)—or how they store and transmit data (security). Obviously, countries have the prerogative to

determine how companies use data, but this again highlights how the focus should be on how companies treat data—and holding them accountable to those standards—rather than where data is stored.

What this shows is that policymakers often misunderstand how the confidentiality of data does not generally depend on what country the information is stored in, but rather only on the measures used to store it securely. Such "inadvertent disclosures" (i.e. security breaches) can happen wherever data is stored (see figure 1). A secure server in India is no different from a secure server in Brazil. Data security depends on the technical, physical, and administrative controls implemented by the service provider, which can be strong or weak, regardless of where the data is stored. For example, in a practice that protects both data privacy and security, some cloud-computing companies have upgraded security controls such that customers retain the keys used to encrypt data before it is uploaded, thereby preventing third parties or cloud companies themselves from accessing their data.[47] This highlights what India should focus on: ensuring that firms managing Indian personal data abide by relevant privacy requirements and use best-in-class cybersecurity measures.

As part of this review, India should identify in advance what metrics it will use to measure the effectiveness of any changes to Indian privacy law; base its approach on evidence to ensure laws and regulations are effective; and consider the economic costs of any piece of privacy legislation or enforcement action, as this law will have a major impact on India's ability to develop a dynamic and innovative digital economy. For example, on the issue of measurement, India should consider metrics for the number and size of data breaches, the amount of financial fraud from identity theft, the number of identity theft complaints, greater cross-border data flows, consumer privacy concerns in federal surveys, and many others could all give a clearer picture of the impact of any changes in law. Without a clear, predetermined understanding of what a "winning" privacy framework would look like, a new set of data privacy rules might simply create higher costs and more market uncertainty that reduce innovation and competitiveness. The "duty of care" approach outlined subsequently aligns with this approach and the overarching principles that responsibility should flow with the data, wherever it is stored.

For example, consistent with the fundamental principles outlined earlier, rather than adopt the "adequacy" standard used by the European Union and copied by others, India should adopt a duty-of-care provision as part of its privacy framework. When it comes to handling data, companies doing business in a country should be responsible for their own actions and the actions of both their agents and business partners, regardless of where they are located. This could be made clear in law by declaring that companies doing business in a country are legally responsible for any failures to protect the personal data of that country's citizens, regardless of whether those failures are the fault of the company in that country, or an affiliate or business partner in another nation. In other words, a country's data protection would travel with the data, regardless of where the data travels. Companies doing business in a given country would then have a strong incentive to assist their business partners outside that country in adhering to relevant national privacy protections, because the firm's citizens and home government could seek remedies for any privacy violations.

This duty-of-care approach to data privacy is shared by most nations, after all. For example, although the United States does not have an "adequacy" standard, companies in the United States need to enact proper data protection measures and safeguards when processing data outside the country, as they remain responsible

for the data regardless of where it is processed. U.S. companies mitigate these risks by stipulating requirements in relevant data handling and processing contracts they implement with other companies. For example, Indian companies operating in the United States must comply with the privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA), which regulates U.S. citizens' privacy rights for health data—even if they move data to Mumbai. And, if a company's affiliate in Mumbai violates HIPAA, then U.S. regulators can bring legal action against the Indian company operating in the United States.

Interoperable privacy frameworks represent the international extension of a duty-of-care approach such that data is still able to flow between different privacy regimes, and a country's data protection rules flow with it. This reflects a central point policymakers need to recognize when dealing with data privacy: Modern technology, especially the Internet, dictates each country's domestic data protection regimes be global in scope and application. The goal for interoperability also reflects the fact that there will be no one global privacy regime. It is no surprise that interoperability is part of the goal of the leading data-protection initiatives, such as at the Organization for Economic Cooperation and Development (OECD) and Asia-Pacific Economic Cooperation (APEC).

Regulatory Oversight and Focusing on Access to Data (Not Where Data is Stored)

The draft Policy's section on "law and order" (page 27) touches upon the broad issue of regulatory oversight and data governance, stating that "access to data for purposes of maintaining and ensuring law and order cannot be over emphasized" and that "participants of the digital economy that have access to the data of Indians must nominate a local representative to be responsible for the affairs of the company in India."

India should not mistakenly believe that data localization and a local office is the only way to enforce data-handling requirements on foreign organizations. This is not the case. While any country can demand extraterritorial application of its laws, it may not always be able to enforce them. This is less likely to be a challenge in the case of privacy and security laws for many foreign firms doing business in another country because their local presence places them within the jurisdiction of that foreign country. For example, many businesses have foreign workers (e.g., sales teams) or foreign assets (e.g., real estate, products, or bank accounts) that give foreign countries viable mechanisms for enforcement of failures to abide by civil or criminal laws. Policymakers have leverage over firms doing business virtually because they can block access to domestic markets, such as by prohibiting local advertising.

Similar to the issue of data privacy, India should place responsibility at the center of its data governance framework when dealing with issues around data and regulatory oversight, such as for data related to financial, payment, and publicly listed firms. Modern cloud computing, which allows transfers of data with the click of a button, enables firms to provide such access, while still allowing firms to move financial data freely in order to provide secure, innovative, and global services. The focus for India's regulatory framework should be the immediate, direct, complete, and ongoing access to a firm's data for regulatory oversight purposes, regardless of where this data is actually stored. Obviously, if a firm is unable to provide authorities with timely access to data, it should face legal penalties. But again, the focus should be on holding firms accountable regardless of where they store data.

Case Study: Avoid Repeating the Reserve Bank of India's Mistaken Approach to Data Governance

The Reserve Bank of India's (RBI) approach to payments data is a case study in what India should avoid in the future. On April 5, 2018, the RBI enacted unnecessary, trade-distorting, and discriminatory data localization requirements for payments data. Despite not providing any evidence of having faced regulatory issues pertaining to access to data, the RBI's notional reasons for data localization were concerns over regulatory oversight and cybersecurity, as the bank cited the need for "continuous monitoring and surveillance" of payments data in order to reduce the risk of data breaches by ensuring payment services use the best global cybersecurity standards.[48]

The brief RBI notice announcing the policy stated, "It is observed that at present only certain payment system operators and their outsourcing partners store the payment system data either partly or completely in the country. In order to have unfettered access to all payment data for supervisory purposes, it has been decided that all payment system operators will ensure that data related to payment systems operated by them are stored only inside the country within a period of 6 months."[49] The data should include the full end-to-end transaction details, and information collected, carried, and processed as part of the message or payment instructions. The RBI set a short deadline for implementation (October 15, 2018), before which it asked companies to provide updates every two weeks. Despite various stakeholders (including the Payments Council of India and the U.S.-India Business Council) criticizing the measure as unnecessary and onerous—and the implementation period being far too short to reconfigure complex IT systems—the RBI persisted and asked for immediate compliance.

At the heart of this regulation's focus on geography is the mistaken belief that data must be stored domestically in order for it to remain secure, private, and accessible to government. If RBI access to data was a legitimate issue, the starting point should be an analysis of the legal framework whereby payment firms provide the RBI with timely access for regulatory oversight. Any legal remedies the RBI considers insufficient should be addressed via policy revisions. As part of this, the RBI should focus solely on the provisions that provide the legal framework so that the RBI has sufficient confidence financial firms are properly managing their data and if need be can provide data on demand. The EC's efforts are a useful reference point for the Central Bank on this issue pertaining to access to data. As part of efforts to build a digital single market, the EC is working to remove barriers to the transfer of company, tax, bookkeeping, and financial data, and asking that member states focus on mandating access.[50] For example, in 2015, Denmark changed its local data storage requirement for accounting data such that companies could store their data anywhere, as long as Danish authorities were given easy access to it on request.[51] This is where the focus should be: putting in place the legal framework to ensure companies provide data to regulatory authorities in a timely manner.

If the RBI is worried that firms will avoid regulatory oversight by simply shifting data overseas, this is similarly mistaken. Similar to data privacy responsibilities, financial firms doing business in India need to be approved by the RBI, which means they must have "legal nexus" in India in order to be put under the RBI's jurisdiction. As such, firms must comply with whatever rules the RBI has on data, regardless of whether they store data in the host country, the home country of the foreign firm, or even a third country. In this way, just as consumer safety and other laws apply to tangible goods that flow in and out of a country as part of

international trade, cybersecurity and other rules apply to data and the financial firms that move and store data in another nation.

The United States' experience with this same issue should be instructive for the RBI and the broader Indian government as it considers regulatory issues that relate to data. The U.S. Treasury and financial regulators recently reconsidered a policy that would have allowed data localization for financial data, but instead enacted a policy framework that focuses on maintaining access to data. U.S. regulators' concerns were based on their experiences in the global financial crisis when they had issues getting access to data in key banks' (i.e., Lehman Brothers') IT systems during bankruptcy proceedings. The U.S. Federal Reserve and Federal Deposit Insurance Corporation's (FDIC's) ability to use and analyze Lehman's IT system and data was reportedly hindered as the bank's network became fragmented, overseas subsidiaries were sold off, some IT systems in overseas subsidiaries were turned off, some key IT staff departed, and restrictions on data flows were imposed due to insolvency filings in other countries—as was the case when the United Kingdom's financial regulator took over Lehman Brothers' European division.[52] This made it difficult for the regulators to access the data needed to unwind positions and ascertain what money was owed to whom.[53]

However, subsequent legal reforms in the United States (e.g., the Dodd-Frank Act, enacted in 2010) have addressed these concerns by focusing on how companies disclose to regulators the way they manage their IT and data as part of regular prudential compliance activities. This means that, in the event of a crisis, regulators know the company will be able to provide the data they want. The law outlined extensive new rules that require "systemically important financial institutions" (SIFIs) to prepare "resolution plans"—also known as "living wills"—that specify a company's strategy for "rapid and orderly resolution in the event of material financial distress or failure of the company."[54] U.S. living wills achieve this by requiring firms to meet stringent requirements about how their IT systems are organized and how data is stored, accessed, and managed on an ongoing basis (as part of periodic compliance activities) in the event of a crisis.[55] India should look to emulate the U.S. review process whereby regulators check IT plans and provide advice to individual firms about how to improve the way they manage and report on their IT and data management systems. If the independent audits identify issues about how firms are organizing and reporting their IT and data systems, the RBI could then issue additional sector-wide advice for all firms. The focus should be on this framework and process, not the location of data storage.

Digital Customs Duties—Avoid Raising Costs and Breaking a Global Consensus

India should avoid making digital goods and services more expensive by enacting customs duties on imports. India should avoid the misguided trap of viewing digital products through a zero-sum lens in comparing these against (falling and insignificant) tariff revenue for some of the analogue versions of these digital products (such as CDs and DVDs).

The draft Policy states:

- **Page 10**—"The push for initiating negotiations on substantive obligations related to e-commerce includes elements like permanently accepting the moratorium on imposing customs duties on electronic transmissions. With increasing digitization, more and more products like books,

music, films, video games, etc. are being traded electronically. By agreeing to the permanent moratorium, countries which have tariff schedules, which allow putting duties on these kinds of products, will give up these rights and lose revenues."

- **Page 10**—"By making the moratorium permanent, and with more and more products now traded digitally in the era of additive manufacturing and digital printing, the GATT schedule of countries will erode and will vanish ultimately. Assuming that all non-agriculture products can be traded electronically, then everything will be traded at zero duty. So, the protection that is available to India, for the nascent industries in the digital arena will disappear at once, and that is an immensely important issue which concerns public policy makers in the developing world."

As to the first point, enacting duties on digital products is unadvisable for many reasons, not least of which is that by raising the price of ICTs such policies undermine a central driver of productivity growth in modern economies (as detailed above). If India were to follow in Indonesia's similarly misguided steps in considering tariffs on digital imports, this could potentially include a broad range of digital products, covering operating system software, smart phone apps, multimedia products (audio, video, or audiovisual), driver data (including for machinery systems), and other software and digital products.[56]

As to the second point, if India were to enact tariffs on products traded digitally, it would contravene and breach the long-standing moratorium among World Trade Organization (WTO) members not to enact duties on the data transmissions that constitute e-commerce. The moratorium was first agreed to in 1998 and has been renewed on a rolling two-year basis, most recently at the end of 2017 (which included India). "Electronic commerce" is generally understood to mean the production, distribution, marketing, sale, or delivery of goods and services by electronic means.[57] In 1998, digital products such as software and e-books were in their infancy, so the moratorium was a rather commendable—and successful—prediction of the digital future of trade and a statement of faith about the need to preemptively protect e-commerce and digital trade from traditional barriers to trade. While WTO members could only imagine what a global digital economy might look like at this stage, they advocated for a mechanism to prohibit tariffs nevertheless, in part recognizing that a core goal of the WTO is to encourage trade and reduce tariffs and duties globally. Digital goods were the latest manifestation thereof.[58]

Data and Competition Policy—Focus on Anti-Competitive Behavior, Not the Amount of Data

India's draft e-commerce policy rightly focuses on the central role of data in today's digital economy. However, it misguidedly points (section 4.8 on page 26) toward a belief that a firm's collection of massive amounts of data and leveraging of network effects is in-and-of itself anti-competitive (which it isn't). Moving forward, Indian policymakers would be wise to instead ensure India's competition policy framework is capable of managing cases where firms engage in anti-competitive behavior, which may involve data, but not simply on the basis that a firm holds large amounts of data.

As ITIF argues in "IP Protection in the Data Economy: Getting the Balance Right on 13 Critical Issues and The Myth of Data Monopoly: Why Antitrust Concerns About Data are Overblown," collecting large amounts of data does not by itself represent a threat to competition.[59] With the increased power and

decreased cost of collecting, transmitting, and storing data, as well as the increase in machine-readable data, more and more companies are using more and more data to help them provide goods and services. The general argument is that the mere act of collecting large amounts of data, such as the vast quantities of personal data collected by social-networking platforms, search engines, and e-commerce sites, gives companies an unfair competitive advantage and that competition policy needs to incorporate this analysis.

To date, U.S. and European regulators have not adopted this line of reasoning (nor should they). While it is true that data can be used in anticompetitive ways, competition policy is capable of dealing with such abuses. In fact, when analyzing allegations of such behavior, it is often helpful to imagine whether agencies would object if the activity complained about involved some input of critical importance other than data. This helps clarify whether the threat to competition is truly due to control of an important resource or to ungrounded fears about the uniqueness of data.

Just like any other important resource, companies may use data in many ways to thwart competition: They can conspire to raise market prices; firms holding major market shares can merge; they can use market power in one sector to unfairly thwart competition in another; or a dominant company can try to extend its position by purchasing an upstream or downstream partner. In each of these cases, existing antitrust law allows regulators to take effective action. But merely having more data than one's rivals does not itself threaten competition any more than having more machines does. And the fear that large amounts of data may create other social problems needs to be addressed to other regulators, not antitrust agencies.

Policymakers in India need to be careful about their approach to data and competition policy, lest they stifle the large social value created by the gathering, analysis, and sharing of data. Innovation often depends on it. Moreover, if regulators began preventing companies from acquiring large amounts of data, this would delay or prevent many important technological advancements. For example, Tesla's self-driving vehicle technology (which faces increased competition from Google, rival car-makers, and others), IBM Watson's ability to diagnose medical illnesses, and the Weather Company's weather predictions would all be impossible without massive amounts of data. Data is also how Google often knows what you are searching for before you finish typing it in, how Facebook connects you with lost friends, and how Waze calculates the best route for drivers to take, all conveniences that consumers already take for granted.

THE IMPACT AND COST OF DIGITAL PROTECTIONISM AND INNOVATION MERCANTILISM

At the heart of the draft Policy's focus on the geography of data is the mistaken belief that digital protectionism is a short cut to high-tech jobs, investment, and innovation. Such a protectionist, import substitution-based approach to digital development is the wrong choice for India, especially given that it's home to a globally competitive services sector that depends on other countries not pursuing exactly these types of data restrictions.

Problematic sections of the Draft policy:

- Page 7—"Development of data-storage facilities/infrastructure is an important vision of the Policy wherein data centres, server farms, towers, tower stations, equipment, optical wires, signal

transceivers, antennae will be granted 'infrastructure status' to facilitate last mile connectivity across urban and rural India. Domestic alternatives of foreign-based cloud services and email facilities are also promoted under the Policy."

- **Page 15**—"At this juncture there is no legal framework that would permit the government to impose restrictions on cross-border flow of data. Without having access to the huge trove of data that would be generated within India, the possibility of Indian business entities creating high value digital products would be almost nil. Domestic technology companies would be merely processing outsourced data work. Further, by not imposing restrictions on cross-border data flow, India would itself be shutting the doors for creation of high-value digital products in the country."

- **Page 16**—"Location of the computing facilities like data centres and server farms within the country will not only give a fillip to computing in India but will also lead to local job creation…. In the future, economic activity is likely to follow data. It is hence vital that we retain control of data to ensure job creation within India. Cloud computing should become an economic activity in India."

- **Page 18**—"Domestic alternatives to foreign-based clouds and email facilities will be promoted. Ways of promoting this could include budgetary support."

The draft policy perpetuates the mistaken belief that if a country restricts data flows, it will gain a net economic advantage from companies that will be forced to relocate data-related jobs to the country.[60] These supposed benefits of data-localization policies are incorrect. While data centers contain expensive hardware (which is usually imported) and create some temporary construction jobs, they employ relatively few full-time technical staff.[61] Data centers are typically highly automated, allowing a small number of workers to operate a large facility. Many next-generation data centers run "next-generation workloads" related to the Internet of Things, robotics, virtual reality, or machine learning, which are often managed using artificial intelligence.[62] In a 2015 review of data center operations across the United States, CBRE Data Center Solutions Group (a U.S. real estate firm) estimated that a typical data center creates between 5 and 30 permanent jobs.[63]

Examples:

- Microsoft's data center in Quincy, Washington had as many as 500 workers on-site at a time during the construction process, but now employs 50 full-time staff to man the center.[64]
- In 2011, a $1 billion data center built by Apple in North Carolina created only 50 full-time jobs and another 250 support jobs in the local community in areas such as security and maintenance.
- Google invested $1.2 billion in a data center in the U.S. state of Oregon in 2016, yet only hired 175 employees.[65]

- In 2018, Facebook started construction on a $750 million data center in the U.S. state of Utah, which will employ 30-50 people full time once completed.[66]

The size and growth of India's digital economy means that market forces will draw data centers to the country. For example, Microsoft launched three cloud data centers in India in September 2015, IBM launched one in October 2015, while Oracle, DigitalOcean, and Amazon have announced plans for data centers.[67] But this has happened without legal requirements as there are competitive advantages to being closer to a growing number of customers (in terms of latency and other services). However, data center operators should be free to make their decision based on market considerations, and not be compelled to setup operations due to government restrictions. India should adopt an attraction, not a compulsion, strategy toward prevailing on IT companies, domestic and foreign alike, to open more data centers in India and reduce the cost of IT services.

Research Shows that Barriers to Data Flows Undermine Firm Competitiveness and Economic Productivity

Meanwhile, the economic benefit from these very limited number of data center jobs are far outweighed by the increased costs of data processing following on from these policies.

At the firm level, barriers to data flows make firms less competitive, as a company will be forced to spend more than necessary on IT services. Companies will likely have to pay more for data-storage services, especially those in smaller countries (which will not naturally be home to a data center). Such barriers also prevent companies from transferring data that's needed for day-to-day activities, such as for human resources, which means companies may have to pay for duplicative services. Likewise, companies may be compelled to spend more on compliance activities, such as hiring a data-protection officer, or putting in place software and systems to get individuals' or the government's approval to transfer data. These additional costs are either borne by the customer or the firm, which undermines the firm's competitiveness (especially for foreign firms who are at some disadvantage vis-a-vis domestic firms) by cutting into profit margins.

This economic impact ripples throughout an economy as barriers to data flows affect data processing and Internet services—or any service that depends on the use of data for delivery, which in today's economy is most. The opportunity cost is that the resources could otherwise go toward hiring new employees or buying new equipment. A growing body of research has examined not only the relationship between cross-border data flows and economic growth but the economic costs engendered by limiting cross-border data flows.

For example, a 2016 Center for International Governance Innovation (CIGI) and Chatham House study found that restrictive data regulations, including forced data localization, increase prices and decrease productivity across a range of economies. The report's econometric study analyzed the negative impact data-protection measures had on 10 downstream sectors (i.e., the users of data or data-related services) and the impact this had on the broader economy in Brazil, China, the European Union, India, Indonesia, Russia, South Korea, and Vietnam.[68] The study first identified and combined common data regulations to use as a proxy, such as full/partial data localization; strict consent for collection, storage, and dissemination of personal data; and user rights of review of stored information. It then estimated the industry impact by calculating the data intensity of downstream sectors, such as telecommunications and information services.[69] It used these

two measures—data regulations and industry-data intensity—to form a joint indicator for a regression analysis to estimate the economy-wide impact via the change in total factor productivity (TFP).[70]

The study used this indictor as a counterfactual to assess the economic impact of actual or proposed data regulations, including localization, in India.[71] As part of this, the study developed a weighted index to compare the severity of data-regulation barriers in each country. It is unsurprising that Russia (4.82) and China (3.88) scored the highest (out of a one to six scale, six being the worst) because of their explicit data-localization measures. India (2.36) is not far behind, due to a mix of data localization and other measures.[72] The regressions showed that data localization and commonly used barriers to data flows decreased TFP, such that a one-standard-deviation change in the joint indicator decreased TFP by 3.9 percent. In the final stage, the study's econometric modeling showed that the lost TFP in downstream sectors, especially in the services sector, reduced GDP by 0.25 percent for India.[73]

Another example is a 2014 European Center for International Political Economy (ECIPE) study, which estimated the economic costs related to proposed or enacted data- localization requirements and related data-privacy and security laws in Brazil, China, the European Union, India, Indonesia, South Korea, and Vietnam.[74] The study examined the effects of recently proposed or enacted legislation (including data localization) in study countries and considered other common regulatory requirements for data protection that increase compliance costs, such as strict consent requirements for data use and transfers, a right for users to review personal data, strict requirements to notify authorities of data breaches, appointing a data-privacy officer, sanctions for noncompliance, and the requirement to provide government access to a business or its customers' data.[75]

The study's econometric model used regulatory and cost indices to analyze the productivity, price, and investment "shocks" from data restrictions and data-localization policies. The model accounted for different levels of data intensity in different sectors to estimate the productivity impact.[76] The study used two scenarios: The first sets a benchmark by examining data-protection regulations in each country, which is built upon in the second scenario by adding data-localization policies. The model assigns weights to the measures to account for different levels of restrictiveness.

The study aimed to analyze the impacts on exports, GDP, and consumer welfare (lost consumption due to higher prices and displaced domestic demand). ECIPE estimates that policies that increase data-processing costs negatively impact economic growth through higher prices on data services. The results are significant and negative. If India enacted economy-wide data localization, the study estimates that higher prices and displaced domestic demand would lead to consumer welfare losses of $14.5 billion for India. Such economy-wide data localization would also reduce domestic investment by an estimated 1.4 percent. Put simply, all major studies conducted on this point are consistent: the Indian economy would be harmed by the introduction of value-destroying data localization policies.

E-COMMERCE, SMALL PACKAGE TRADE, AND TRADE FACILITATION

The draft Policy should be commended for focusing on the "traditional" conceptualization of e-commerce, in terms of a digital platform acting as a marketplace for physical goods (often low-value items) for buyers and

sellers from different parts of the same country or from different countries around the world. This small package-focused e-commerce approach raises issues about logistics and trade facilitation both within a country and between countries

Some of the relevant sections of the draft Policy:

- **Page 8**—"Domestic digital economy is sought to be facilitated by creation of industrial standards for smart devices and IoT equipment, automation of logistics sector, adoption of Customs Electronic Data Interchange (EDI) platform, Customs validation for availing benefits from schemes like duty drawbacks, minimizing procedures and documentation, conducting cluster specific programmes for exporters to increase awareness on procedural formalities, inclusion of eCommerce in the proposed National Integrated Logistics Plan and continued focus on Digital India initiatives."
- **Page 8**—"Indian domestic manufacturers/MSMEs/start-ups/sellers/retailers stand to benefit from the enhanced visibility provided by e-commerce platforms. Improved infrastructure, lower selling price and reduced costs associated with marketing and outreach of products over a digital platform contribute to promoting online sales. Transaction costs adversely affect MSMEs and start-ups more than the big corporations. Therefore, the Policy proposes removal of application fee for claiming export benefits. Likewise, possibilities of avoiding obtaining the BRC are proposed to be explored by DGFT in consultation with RBI. This would reduce the related costs for MSMEs and start-ups. The benefits of end-to-end delivery offered by private logistics companies should be brought to the MSMEs and startups by leveraging the wide network of India Post to negotiate lower costs with international freight carrier companies."
- **Page 31**—"e-commerce will also be included in the National Integrated Logistics Plan being prepared by the Department of Commerce, which would focus on faster delivery with emphasis on lower costs."
- **Page 34**—"Manufacturers, sellers, traders, MSMEs or start-ups adopt business models to facilitate online sales in order to expand their outreach beyond geographical limitations. MSMEs and other domestic manufacturers are based across the country but shipments via courier for e-commerce exports are accepted by airports in Delhi, Mumbai and Chennai only. Therefore, implementation of EDI mode at courier terminals shall be fast tracked to facilitate quicker and easy dispatch of export consignments."

From a trade policy perspective, the Policy raises a number of important issues to supporting small-package trade involving buyers and sellers from different countries. This deserves special attention as the Internet enables micro, small, and medium-sized businesses ("MSMEs" or "SMEs") to access global markets unlike ever before, especially via use of their own websites or platforms to sell small packages. Addressing barriers to SME-based small packages trade holds broader economic significance—SMEs that engage in trade employ more people, pay higher wages, achieve higher sales, and are more productive than SMEs that do not.[77] Exporting SMEs also have a higher chance of surviving. Exporting helps SMEs learn, innovate, diversify sources of revenue, improve capacity utilization, and improve overall competitiveness. In addition, helping

SMEs diversify their exports drives further firm productivity.[78] However, these modern businesses still face traditional market barriers: the cost, time, and ease of getting these packages to their customers in another country. Trade liberalization has reduced tariffs and quotas, propelling dramatic growth in trade in recent decades, but it's now at a point in many countries that logistics costs are greater deterrents to trade than remaining tariffs.[79]

Trade facilitation issues matter for e-commerce as poor or weak infrastructure, custom procedures, and logistics competition has a direct impact on trade costs, which especially for SMEs, can quickly erode profits from exports. SMEs don't have the scale, resources or administrative capacity to navigate legal and regulatory issues across multiple jurisdictions. Time equals money for small packages trade, and when the wait times for customs clearances in India are long, these costs become a significant barrier to trade. Each day adds considerable costs— studies estimate that each extra day a good is in transit is equivalent to an 0.6 to 2.3 percent ad valorem tariff.[80] Higher trade costs are one of the reason why there are not more firms exporting a greater variety of goods to more foreign markets in the rest of the world.[81] Thereby, improving the cost, speed, and efficiency of border procedures—whether through capacity building, harmonization, digitalization, or transparency—addresses a real-world barrier to digital trade.

The Policy rightly looks into the issues of adopting electronic data interchanges for online customs clearances and integrating IT systems between various government agencies as part of broader efforts to improve customs facilitation for packages coming into and out of India. India has already taken a step in the right direction in signing and implementing the WTO's Trade Facilitation Agreement.[82] India should do a whole-of-government review of the various factors that inhibit greater small package exchange within India and between India and the rest of the world, including issues such as: reviewing remaining WTO Trade Facilitation Agreement provisions; reviewing transparency requirements so that buyers/sellers (in any given country) understand the rules and regulations in place, and are able to access these online, in order to be able to comply with them and pay any applicable duties/taxes; review what forms can be digitalized and standardized such as Know Your Customer forms; review coordination mechanisms for relevant trade facilitation issues at the national level and between the national government and state governments; and review market access for logistics services, such as express delivery services, as foreign providers can spur greater competition and efficiency in local markets and act as a facilitator for local exporters to get their goods to customers around the world.

E-COMMERCE, INTELLECTUAL PROPERTY, AND VOLUNTARY AGREEMENTS

India's draft Policy rightly recognizes that intellectual property is a critical part of a successful digital economy and that voluntary agreements between different stakeholders can be an effective policy to help support the sale of legal content and reduce digital piracy. The rise of digital trade makes including intellectual property protection and enforcement even more of an imperative as the Internet not only makes it much easier and cheaper to distribute legal digital content, but it also makes it easy to steal. This extends to copyright for content like movies, music, and video games. To be effective, e-commerce requires robust intellectual property (IP) protections, because without them producers will be less able to sell their products and services. A 2017 empirical and literature review of copyright enforcement in the digital age identified and reviewed 26

peer-reviewed journal articles studying the economic harm caused by piracy, finding that 23 of them found that piracy causes significant harm to legal sales.[83]

Some relevant provisions from the draft Policy:

- **Page 22**—"Intermediaries shall put in place measures to prevent online dissemination of pirated content. Intermediaries shall identify 'trusted entities', whose complaints are resolved on priority. The identification of trusted entity and anti-piracy measures shall be done on a voluntary basis."

- **Page 22**—"A body of industry stakeholders will be created that shall identify 'rogue websites'. Rogue website would refer to those that host predominantly pirated content. After verification, these rogue websites shall be included in the "Infringing Websites list'. This shall invite the following: a) Internet service providers shall remove or disable access to the websites identified in the IWL within set time-lines. b) Rogue websites earn their revenues through online payments made based on a subscription or advertisement revenue models. Such payments have to be routed through Payment Gateways, which shall not permit flow of payments to or from such rogue websites. c) Search Engines shall take necessary steps to remove websites identified in the IWL, in their search results. d) Advertisers or advertising agencies shall not host any advertisements on the websites identified in the IWL."

Countries face the challenge in putting in place a framework to support an open, competitive, and innovative digital economy in legal digital content. India needs to conduct a holistic assessment of the broad policy toolbox it has at hand to do this. Countries need to enact policies that enable a robust ecosystem of legal service providers in order to make it easier and cheaper for users to get legal digital content online instead of using piracy sites. At the same time, countries need legal remedies to combat piracy activity taking place domestically, including prosecuting the operators of large-scale piracy websites hosted in India. At the international level, many countries (including India) are creating a legal framework to allow rightsholders to get Internet service providers (ISPs) to block access to websites engaged in the large-scale distribution of copyright infringing material because this is one of the few means available to authorities responding to illegal services and materials hosted abroad.[84] This is important, given the growing and vibrant nature of India's content industry.

Voluntary agreements can play a supporting role alongside these other policies in helping fight digital piracy at home. India has the benefit of being able to review and learn from what arrangements have been established between stakeholders in other countries. Voluntary agreements differ by country, membership, and issue. Such industry-led voluntary agreements between different players involved in the digital economy (rightsholders, Internet intermediaries, payment providers etc.) are still a relatively new mechanism that can complement legislative efforts to support the market in legal content and reduce the availability of illegal content. It important that as India looks to encourage stakeholders to setup similar arrangements that they do so within a clear framework that is transparent, non-discriminatory (between domestic and foreign stakeholders and targeted piracy websites), and involves a notice, dispute, and recourse mechanism (e.g. for targeted websites to be removed from an infringing website list).

For example, in the United States, during the Obama administration, the U.S. Department of Commerce's Internet Policy Taskforce encouraged stakeholders to take part in existing initiatives and to develop others relevant to their own sectors.[85] This has continued in the Trump administration, which is engaging and working with the private sector and other stakeholders as one part of its four-part strategic approach to IP enforcement.[86] In September 2018, the U.S. Intellectual Property Enforcement Coordinator asked for input regarding the U.S. government's intellectual property enforcement efforts in developing a new three-year Joint Strategic Plan on Intellectual Property Enforcement. Voluntary agreements have been part of past IPEC strategic plans.[87]

Similarly, the European Commission has started using voluntary agreements as part of its broader efforts to help fight digital piracy and to create a Digital Single Market.[88] For example, as part of the European Commission's 'follow the money' approach to intellectual property enforcement, it developed a Memorandum of Understanding (MoU) on online advertising and intellectual property rights (detailed below). As Vice President of the European Commission Andrus Ansip stated at the signing, "MoUs are a key pillar in the work on the enforcement of IPRs."[89] This represents a key development as the enforcement of copyright online has stereotypically been characterized by a lack of shared approaches between countries at the European Union level.

Example: The United States: Domain Name Registries—Trusted Notifier Programs

As it relates to the draft Policy's mention of "trusted entities," voluntary agreements in the domain name registry sector perhaps provide a useful reference for Indian policymakers. There are several voluntary initiatives that involve rightsholders and domain name stakeholders setting up so-called "Trusted Notifier" programs to streamline the process to respond to notices from the former to the later about cases where large-scale pirate sites have registered domains with their service, which contravene the domain name registry operator's anti-abuse and acceptable use guidelines.

For example, on February 9, 2016, the Motion Picture Association of America (MPAA) announced the first of these Trusted Notifier programs with Donuts, the largest operator of new domain name extensions (such as .MOVIE, .THREATRE, or .COMPANY, and over 200 other naming options).[90] The president of the Internet Corporation for Assigned Names and Numbers (ICANN)—the private organization that governs the Internet's domain name system—welcomed the agreement.[91] The Donuts-MPAA agreement shows how private-sector stakeholders can come together to address online piracy and create a win-win scenario for all partners.[92] For Donuts, the agreement protects its brand by ensuring that its domains are legitimate and law-abiding contributors to the digital environment. For MPAA, the agreement provides a clear path toward the removal of infringing sites and material, albeit with the responsibility to fulfill a number of clearly defined and detailed steps it has to make in presenting its case. In the first year, 12 domain names were submitted seven of which were suspended or deleted by the registrar, three were suspended by Donuts, and one was addressed by the hosting provider.[93]

Following this, on May 13, 2016, MPAA announced a second Trusted Notifier agreement with Radix, another domain name registry operator, to ensure that websites using domains operated by Radix are not engaged in large-scale commercial piracy.[94] It's a first in that it's with an operator outside the United States.

Radix has launched seven new domain extensions, including .online, .tech, .space, .website, .press, .host, and .site. The agreement, which is similar to the one with Donuts, imposes strict standards for such referrals, including that they be accompanied by evidence of clear and pervasive copyright infringement, and a representation that the MPAA has first attempted to contact the registrar and hosting provider for resolution.

Example: Infringing Website Lists and "Follow the Money" Efforts to Target Piracy Profits

India's draft Policy is right to be looking at "follow the money" efforts to fight digital piracy by cutting off pirates' ability to earn money from advertising. Similar to India, many countries have or are considering following the United Kingdom's model of using an updated infringing website list (IWL) to help ensure reputable brands and advertising agencies don't place ads on piracy websites.

Initially developed in 2013, the United Kingdom setup a voluntary arrangement—called "Operation Creative"—between the City of London Police Intellectual Property Crime Unit (PIPCU) and various advertising and rightsholder stakeholders to identify websites engaged in copyright infringement and take remedial measures targeting them.[95] PIPCU is funded by the United Kingdom's Intellectual Property Office. As part of this, rightsholders identify and report copyright-infringing websites to PIPCU, which then evaluates and verifies that the websites are infringing copyright. PIPCU then contacts site owners in an attempt to give them the opportunity to engage with the police and correct their behavior. If the website fails to engage and comply with the police, then PIPCU moves to remedial measures, such as contacting the domain registrar to seek suspension of the site, advertisement replacement, and disrupting advertising revenue through the use of an Infringing Website List (IWL).

The PIPCU's IWL is the first of its kind in that it is an online portal containing an up-to-date list of copyright-infringing sites, identified, and evidenced by the creative industries and verified by the City of London Police unit. The head of PIPCU estimates that a single website owner involved in large-scale piracy can make as much as $84,200 a year from advertising.[96] Operation Creative supports broader follow-the-money efforts in that it's available to those agencies involved in the sale and trading of digital advertising with the goal of allowing them to voluntarily cease advert placement on these illegal websites. The program has been very successful. A March 2017 report from Whitebullet (a global data company) showed a 64 percent decrease in advertising from the UK's top ad spending companies on copyright-infringing websites (comparing 205 websites on the Infringing Website List in both January 2016 and January 2017).[97] Another study from Whitebullet in June 2017 showed an 87 percent drop in advertising from licensed gambling operators on illegal sites that infringe copyright laws over the previous year.[98]

Countries around the world have started adopting IWLs as part of their efforts to target digital piracy. Elsewhere in Europe, Denmark setup an IWL based on websites determined by Danish courts as facilitating copyright infringement. The Danish government helped facilitate an MOU/code of conduct between the various Internet stakeholders so that ISPs block access to these sites and advertisers don't show ads on these sites.[99] In other countries, like Italy, Germany, Spain, and Denmark, various announcements have been made about tackling suspected ad-funded IP infringement.[100] In Asia, Indonesia (October 2017), Malaysia (October 2017), Hong Kong (December 2016), Vietnam, and Taiwan (September 2017) have setup IWLs.[101] In Hong Kong, on October 3, 2017, the Hong Kong Creative Industries Association (HKCIA) reported that

Hong Kong's "Infringing Website List" (IWL) Scheme (launched in December 2016) resulted in the removal of advertisements on infringing websites by 50 brands in Hong Kong and reduced traffic of a number of infringing websites by 14 percent on average. This is progress, given online advertising spending in Hong Kong in 2017 was estimated to be HK$5.72 billion, and approximately 30 percent went to these infringing websites.[102]

INTELLECTUAL PROPERTY AND SOURCE CODE—FORCED DISCLOSURE AS A BARRIER TO TRADE AND INNOVATION

Source code—the instructions that programmers write to make a computer program run—enable technology to do the amazing things it does. For companies developing software, protecting source code is necessary to prevent other entities from stealing and free riding on the large research and development costs associated with software development. Source code is increasingly at the heart of cutting-edge firms' competitive advantage, but, being digital, it's at heightened risk of duplication. The draft Policy's forced source code disclosure rules misguidedly focuses on short-term tech transfer goals instead of the longer-term benefits that come from incentivizing firms (whether domestic or foreign) to develop and deploy cutting-edge software and software-embedded products in India.

India's draft Policy contains a number of problematic provisions related to source code:

- Page 10—"During negotiations, policy space must be retained to seek disclosure of source code for facilitating transfer of technology and development of applications for local needs as well as for security."

- Page 26—"In continuation, it is also important for the Government to reserve its right to seek disclosure of source code and algorithms. There will be a greater reliance on AI in decision making in future where parts of the process will become 'AI-fied'. Decisions will need to be explained. There is a need to strike a balance between commercial interests and consumer protection issues, as well as issues of larger public concern, like preventing racial profiling and maintaining constitutionally mandated rights, such as the right to equality."

Forced source code disclosure would act as a major deterrent to foreign tech firms considering entering India or using India for product development, as it would mean that the considerable time and money they invest in research and development could potentially be worthless if Indian authorities pass it to local competitors. Many companies view their source code as their "crown jewels" precisely because competitors do not have access to the source code. They're crown jewels because, as with certain types of software, market dynamics mean that product replacement is very quick, meaning that software firms rely on being the first into the market to capture returns from their research and development activities. Losing critical first-to-market advantage can contribute to overall loss of profitability and could mean the loss of entire product or business lines to competitors. Just as the lack of general intellectual property protections affect foreign investment, trade, and knowledge-transfers, a lack of trade secret protections will increasingly affect how firms trade and operate overseas, especially with regard to a firm's most sensitive intellectual property assets. It would also lead to retaliation against Indian software firms, requiring them to turn over source code to other nations.

Moreover, such policies impose significant reputational harm on India, possibly making it less likely for foreign customers to want to buy from Indian IT service companies.

Forced source code disclosure will likely dissuade foreign firms from entering India (or if they do, not using their most cutting-edge technology as they want to reduce potential risks), which thereby prevents local firms from accessing the most innovative tech services and products. Furthermore, forcing foreign firms to choose between turning over their most valuable asset—their source code—to the government or abandoning the market acts as a barrier to trade. This is exactly why the United States and European Union, along with Japan and the other ten-member countries of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) trade agreement, have agreed to rules that specifically prohibit forced source code disclosure as they recognize that it constitutes a barrier to trade, while allowing narrowly defined exceptions for certain scenarios.[103]

An example of the risk posed by forced source code disclosure is to encryption, which plays an often-overlooked role in today's digital economy. Encryption—the technology many companies use to secure high-tech goods and digital services from unauthorized access—is at the forefront of competition in IT goods and services. Over the last few decades, researches have steadily gotten better at securing data, especially by using encryption, and companies have integrated these advancements into their goods and services to improve security for consumers and businesses. Because proprietary security measures that use encryption represent intangible software that is embedded in goods or services, enterprises' source code—the lines of computer code at the heart of software—is susceptible to theft and replication, and therefore relies on intellectual property protections. As many of these products involve high fixed costs for research and development to bring the first copy to market, but low marginal costs in subsequent copies, encrypted products and services represent an attractive target for foreign governments trying to collect and pass along the intellectual property to help local firms.[104]

India's draft Policy also raises the potential for forced source code disclosure for regulatory purposes. Governments or courts should obviously be allowed to review source code as part of specific investigations and legal proceedings that involve source code where there is a legitimate concern that particular laws have been broken and where there are particular harmful outcomes, but not for the purpose to steal the code (i.e., the focus should be ex post on the outcome involving the technology and the source code, not in some ex ante focus on the source code itself). Using an analogy, governments do not require food producers to disclose their secret recipes despite the fact that these could obviously impact public health, instead, they wait until there is a particular event before investigating the cause. The same approach should apply to source code.

India should not only avoid forced source code disclosure but move to improve trade secret protections in order to support innovation. The shift to a knowledge- and services-based economy means that the strength and competitiveness of domestic firms will increasingly depend upon their know-how and intangible assets, such as is embodied in trade secrets and source code. Source code is protected by WTO trade rules requiring governments to protect commercial trade secrets, but the Trade-Related Aspects of Intellectual Property (TRIPS) rules, while providing an important baseline, are far from global best practice.[105] India should look to the United States and Europe for the model framework for trade secrets. In 2016, the United States enacted the Defend Trade Secrets Act (DTSA), which created a new, private federal civil action for "an owner

of a trade secret that is misappropriated … if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce."[106] Similarly, the European Union released a directive in June 2016 to improve and harmonize trade secret protections across its member countries.[107] Importantly, both the United States and European Union have enacted complementary legal changes that relate to the cyber-component of trade secret theft by enacting laws that make it a crime to access a computer without authorization or for a user to exceed their authorized access.[108]

CONCLUSION

The draft Policy contains some laudable policy proposals and a strong recognition as to the increasingly critical role data and digital technologies play in today (and tomorrow's) economy and society. However, it also includes a range of misguided and harmful policy proposals that together reflect a short-term, sometimes mercantilist approach to digital development that will detract from India's ability to benefit from data-driven innovation, increase the cost of key capital goods (ICTs), likely lead to broad economic inefficiencies, and cause reputational harm that will damage India's attractiveness as a location for foreign direct investment, trade, and data-focused research and development. Despite their possible potential to produce some short-term employment and economic gains, these policies ultimately lead to far worse adverse consequences. Such a digital mercantilist approach is fundamentally unsustainable, in part because it engenders reciprocal protectionist policies by other countries—which undermines the global economic order and lowers levels for global economic growth that otherwise benefits India, and all nations. These policies will also raise the costs and reduce the quality of IT goods and services available in India, thereby reducing IT adoption by Indian organizations and consumers, thereby reducing productivity growth. More broadly, India should adopt an attraction, not a compulsion approach, to the modern ICT and digital economy and should focus on spurring broad based digital adoption, rather than mercantilist based digital industry development. Especially with countries like China continuing to persist in the blatant application of mercantilist policies, an Indian welcome mat for global digital commerce would make it a highly attractive location for international investment.

ANNEX

The National E-Commerce Policy ("the Policy") states that "While Digital India is already unfolding, its pace needs to be accelerated, and innovation and enterprise need to be encouraged inclusively by providing a facilitative ecosystem for stimulating the digital economy." The overall objective of the Policy is to prepare and enable stakeholders to fully benefit from the opportunities that would arise from progressive digitalization of the domestic digital economy. The Policy also seeks to identify the path to achieve this goal through a multi-pronged approach, including the following: creating a facilitative regulatory environment for growth of e-commerce sector; empowering domestic entrepreneurs; encouraging Make in India; safeguarding interests of the consumers; leveraging access to data; mainstreaming the segments of our economy, hitherto having limited access to the digital ecosystem (MSMEs, vendors, traders etc.), by empowering them through skilling and providing institutional support to familiarize them with technology; promoting domestic research and development in digital innovation in order to foster homegrown alternate, cheaper, and efficient service providers suited for the Indian market, including those in digital payment processes, like RuPay and BHIM; enabling domestic players in the Indian market to be sustainable in the digital economy; and stimulating the participation of micro, small and medium enterprises, start-ups, and traders in the digital economy.

Provisions of concern:

- **Page 8**—The increasing importance of data warrants treating it at par with other resources on which a country would have sovereign right. It is said that data is the new oil. Therefore, just like oil or any other natural resource, it is important to protect data, prevent its misuse, regulate the use and processing of data and address the concerns related to privacy and security. The Policy recognises the importance of data while enabling the domestic industry to benefit from the advantages and opportunities created by electronic commerce.

- **Page 14**—Would an individual be expected to pay the company for access to his own data? Would a Government be willing to pay private corporations for data about its citizens? These are crucial questions in determining what the Indian data regime should look like. The data of a country, therefore, is best thought of a collective resource, a national asset, that the government holds in trust, but rights to which can be permitted. The analogy of a mine of natural resource or spectrum works here. India and its citizens have a sovereign right to their data. This right cannot be extended to non-Indians (the same way that non-Indians do not have any prima facie right or claim to, say, an Indian coal mine). This understanding flows from the acknowledgement that data about an Indian, is his/her own… National data of various forms is a national resource that should be equitably accessed by all Indians. The same way that non-Indians do not have access to the national resources on the same footing as Indians, non-Indians do not have equal rights to access Indian data. However, access to it can be negotiated, in national Interest…. Thus, the e-commerce policy is about how best to exploit this national resource, for maximizing growth and for delivering greatest benefits to all sections of society.

- **Page 15**—At this juncture there is no legal framework that would permit the government to impose restrictions on cross-border flow of data. Without having access to the huge trove of data

that would be generated within India, the possibility of Indian business entities creating high value digital products would be almost nil. Domestic technology companies would be merely processing outsourced data work. Further, by not imposing restrictions on cross-border data flow, India would itself be shutting the doors for creation of high-value digital products in the country.

- Page 16—A legal and technological framework to be created that can provide the basis for imposing restrictions on cross-border data flow from the following specified sources: Data collected by IoT devices installed in public space; and b) Data generated by users in India by various sources, including ecommerce platforms, social media, search engines etc. The legal and technological framework would also provide basis for sharing the data collected by IoT devices under (a) above with domestic entities for use in research and development for public policy purposes.

- Page 16—A business entity that collects or processes any sensitive data in India and stores it abroad, shall be required to adhere to the following conditions: a) All such data stored abroad shall not be made available to other business entities outside India, for any purpose, even with the customer consent; b) All such data stored abroad shall not be made available to a third party, for any purpose, even if the customer consents to it; c) All such data stored abroad shall not be made available to a foreign government, without the prior permission of Indian authorities; d) A request from Indian authorities to have access to all such data stored abroad, shall be complied with immediately; e) Any violation of the conditions mentioned above shall face the prescribed consequences (to be formulated by the Government).

ENDNOTES

1. India's Department for Promotion of Industry and Internal Trade, *Draft National e-commerce Policy for Stakeholder Comments* (New Delhi: India's Ministry of Commerce and Industry, March, 2019), https://dipp.gov.in/whats-new/draft-national-e-commerce-policy-stakeholder-comments.
2. Daniel Castro, "The False Promise of Data Nationalism" (The Information Technology and Innovation Foundation, December, 2013), http://www2.itif.org/2013-false-promise-data-nationalism.pdf.
3. McKinsey Center for Business and Technology, "Perspectives on Digital Business" (Industry paper, January 2012), https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/BTO/PDF/MCBT_Compendium_Perspectives_on_Digital_Business.ashx.
4. Daniel Castro and Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries" (Information Technology and Innovation Foundation, February 2015), http://www2.itif.org/2015-cross-border-data-flows.pdf.
5. National Board of Trade Sweden, "No Transfer, No Trade—the Importance of Cross-Border Data Transfers for Companies Based in Sweden" (Stockholm, Sweden: National Board of Trade Sweden, January 2014), http://unctad.org/meetings/en/Contribution/dtl_ict4d2016c01_Kommerskollegium_en.pdf.
6. James Manyika, Susan Lund, Jacques Bughin, Jonathan Woetzel, Kalin Stamenov, and Dhruv Dhingra, "Digital Globalization: The New Era of Global Flows" (McKinsey Global Institute, February 2016), http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows.
7. "Information technology/business process management (IT-BPM) sector in India as a share of India's gross domestic product (GDP) from 2009 to 2017," Statista Portal website, accessed March 7, 2019, https://www.statista.com/statistics/320776/contribution-of-indian-it-industry-to-india-s-gdp/.
8. "IT & ITeS Industry in India," India Brand Equity Foundation website, access March 7, 2019, https://www.ibef.org/industry/information-technology-india.aspx.
9. Ibid.
10. Castro, "The False Promise of Data Nationalism."
11. Robert Atkinson and Ben Miller, "A Policymakers Guide to Spurring ICT Adoption" (Information Technology and Innovation Foundation, 2015), http://www2.itif.org/2015-policymaker-ict-adoption.pdf.
12. Robert Atkinson, "How ICT Can Drive Growth in Emerging Economies, *Innovation Files,* August 10, 2015, https://www.innovationfiles.org/ict-can-drive-growth-emerging-economies/.
13. Jason Dedrick, ViJay Gurbaxani, and Kenneth L. Kraemer, "Information Technology and Economic Performance: A Critical Review of the Empirical Evidence," ACM Computing Surveys 35, no. 1 (March 2003), 1.
14. For several of the numerous literature surveys, see: Mirko Draca, Raffaella Sadun, and John van Reenen, "Productivity and ICT: A Review of the Evidence" (discussion paper no. 749, Centre for Economic Performance, August 2006), http://eprints.lse.ac.uk/4561/; Tobias Kretschmer, "Information and Communication Technologies and Productivity Growth: A Survey of the Literature," OECD Digital Economy Papers, no. 195 (2012), http://dx.doi.org/10.1787/5k9bh3jllgs7-en; M. Cardona, T. Kretschmer, and T. Strobel, "ICT and Productivity: Conclusions from the Empirical Literature," Information Economics and Policy 25, no. 3 (September 2013): 109–125, doi:10.1016/j.infoecopol.2012.12.002.
15. Jack E. Triplett and Barry P. Bosworth, "Productivity Measurement Issues in Services Industries: 'Baumol's Disease' has Been Cured," FRBNY Economic Policy Review 9, no. 3 (2003): 23–33; see also Carol A. Corrado et al., "Sectoral Productivity in the United States: Recent Development and the Role of IT," Productivity Measurement and Analysis (OECD Publishing, 2008), https://www1.oecd.org/std/productivity-stats/44516351.pdf#page=437; Sophia P. Dimelis and Sotiris K. Papaioannou, "Technical Efficiency and the Role of ICT: A Comparison of Developed and Developing Countries," Emerging Markets Finance & Trade 47 (July 2, 2011): 40–53, doi:10.2753/REE1540- 496X4704S303; Jason Dedrick, Kenneth L. Kraemer, and Eric Shih, "Information Technology and Productivity in Developed and Developing Countries," *Journal of Management Information Systems* 30, no. 1 (July 1, 2013): 97–122, doi:10.2753/MIS0742-1222300103).

16. P.D. Kaushik and Nirvikar Singh, "Information Technology and Broad-Based Development: Preliminary Lessons from North India" (working paper no. 522, UC Santa Cruz Economics, July 2002), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=344830.

17. Ben Miller and Robert Atkinson, "Digital Drag: Ranking 125 Nations on Taxes and Tariffs on ICT Goods and Services" (Information Technology and Innovation Foundation, October 24, 2014), https://itif.org/publications/2014/10/24/digital-drag-ranking-125-nations-taxes-and-tariffs-ict-goods-and-services.

18. Stephen Ezell, "A Modi Administration Report Card on the Eve of His Visit to the United States," *Innovation Files*, September 25, 2014, http://www.innovationfiles.org/a-modiadministration-report-card-on-the-eve-of-his-visit-to-the-united-states/.

19. Stephen J. Ezell and Robert D. Atkinson, "The Indian Economy at a Crossroads" (Information Technology and Innovation Foundation, April 2014), 49-50, https://itif.org/publications/2014/04/21/indian-economy-crossroads.

20. Asian Productivity Organization (APO), *APO Productivity Databook 2012* (APO, 2012), 63, http://www.apo-tokyo.org/publications/files/ind_APO_Productivity_Databook_2012.pdf.

21. Ibid.

22. Ibid.

23. The Conference Board, "Total Economy Database, Summary Statistics 1966-2013" (The Conference Board, January 2013), 10, http://www.conference-board.org/data/economydatabase/.

24. For example, in the financial sector, companies use sophisticated analytics and large datasets to prevent fraud as well as to improve and expand their lending services. Daniel Castro and Joshua Misra, 100 Data Innovations, (Center for Data Innovation, January 23, 2014), https://www.datainnovation.org/2014/01/100-data-innovations/; Daniel Castro and Travis Korte, Data Innovation 101, (Center for Data Innovation, November 4, 2013), http://www2.datainnovation.org/2013-data-innovation-101.pdf; Nick Wallace, "5 Q's for David Hand, Emeritus Professor at Imperial College, London", (Center for Data Innovation, January 30, 2017), https://www.datainnovation.org/2017/01/5-qs-for-david-hand-emeritus-professor-at-imperial-collegelondon/.

25. Daniel Castro and Travis Korte, "Data Innovation 101: An Introduction to the Technologies and Policies Supporting Data-Driven Innovation" (Center for Data Innovation, November 4, 2013), http://www2.datainnovation.org/2013-data-innovation-101.pdf.

26. Nick Wallace and Daniel Castro, "The State of Data Innovation in the EU" (Information Technology and Innovation Foundation, October 10, 2017), https://itif.org/publications/2017/10/10/state-data-innovation-eu.

27. Nick Wallace, "Double Consent Rule for Sharing Data Would Be Useless", (Center for Data Innovation, October 31, 2016), https://www.datainnovation.org/2016/10/double-consent-rule-for-sharing-datauseless/.

28. Nick Wallace, "New EU Cookie Law Hurts Ad-Supported Industries (Like Journalism) Without Offering More Privacy", (Center for Data Innovation, March 20, 2017), https://www.datainnovation.org/2017/03/eu-policymakers-shouldovercome-their-fear-of-cookies/; Nick Wallace, "EU's Right to Explanation: A Harmful Restriction on Artificial Intelligence", TechZone360, January 25, 2017, http://www.techzone360.com/topics/techzone/articles/2017/01/25/429101-eus-right-explanation-harmfulrestriction-artificial-intelligence.htm; Nick Wallace, "EU's eCall regulation sacrifices safety for privacy", EurActiv, February 7, 2017, https://www.euractiv.com/section/digital/opinion/eus-ecall-regulation-sacrifices-safety-forprivacy/; Nick Wallace "Overzealous EU data protection regulations are more likely to take your job than a robot", City A.M. March 2, 2017, http://www.cityam.com/260087/overzealous-eu-data-protection-regulations-more-likelytake.

29. Nick Wallace, "European Commission Should Stand Firm on Free Data Flows", (Center for Data Innovation, March 8, 2017), https://www.datainnovation.org/2017/03/european-commission-should-stand-firm-on-free-data-flows/; Nick Wallace, ""Double Consent" Rule for Sharing Data Would Be Useless", (Center for Data Innovation, October 31, 2016), https://www.datainnovation.org/2016/10/double-consent-rule-for-sharing-data-useless/.

30. Surabhi Agarwal, "Internet users in India expected to reach 500 million by June: IAMAI," *The Economic Times,* February 20, 2018, https://economictimes.indiatimes.com/tech/internet/internet-users-in-india-expected-to-reach-500-million-by-june-iamai/articleshow/63000198.cms.

31. "Smart Cities Mission, Ministry of Housing and Urban Affairs website, accessed March 8, 2019, "http://smartcities.gov.in/content/; McKinsey Global Institute, "India's Technology opportunity: Transforming work, empowering people" (McKinsey Global Institute, December 2014), https://www.mckinsey.com/~/media/mckinsey/industries/high%20tech/our%20insights/indias%20tech%20opportunity%20transforming%20work%20empowering%20people/mgi%20india%20tech_full%20report_december%202014.ashx.
32. McKinsey Global Institute, "India's Technology opportunity: Transforming work, empowering people."
33. Devika Singh, "Over 50,000 jobs in data science, machine learning vacant in India: Report," *Business Today,* October 16, 2018, https://www.businesstoday.in/latest/trends/jobs-in-data-science-machine-learning-vacant-in-india/story/285446.html.
34. Rakesh Mohan and Anu Madgavkar, "Labour in India: Quality of quantity counts," *The Economic Times,* July 21, 2017, https://economictimes.indiatimes.com/blogs/et-commentary/labour-in-india-quality-of-quantity-counts/.
35. India's Department for Promotion of Industry and Internal Trade, *Draft National e-commerce Policy for Stakeholder Comments.*
36. Daniel Castro, "The False Promise of Data Nationalism."
37. Stephen Ezell and Robert Atkinson, "The Middle Kingdom Galapagos Island Syndrome: The Cul-De-Sac of Chinese Technology Standards" (Information Technology and Innovation Foundation, December 15, 2014), https://itif.org/publications/2014/12/15/middle-kingdom-galapagos-island-syndrome-cul-de-sac-chinese-technology.
38. India's Department for Promotion of Industry and Internal Trade, *Draft National e-commerce Policy for Stakeholder Comments.*
39. Donald E. Purcell, "Strategic Standardization Overview" (presentation, Catholic University School of Engineering, Washington, D.C., May 18, 2011).
40. Daniel Castro and Joshua New, "10 Policy Principles for Unlocking the Potential of the Internet of Things" (Center for Data Innovation, December 4, 2014), http://www2.datainnovation.org/2014-iot-policy-principles.pdf.
41. Daniel Castro, "The Rise of Data Poverty in America" (Center for Data Innovation, September 10, 2014), http://www2.datainnovation.org/2014- data-poverty.pdf.
42. Daniel Castro and Travis Korte, "A Catalog of Every 'Harm' in the White House Big Data Report," Center for Data Innovation, July 15, 2014, http://www.datainnovation.org/2014/07/a-catalog-of-every-harm-in-thewhite-house-big-data-report/.
43. India's Department for Promotion of Industry and Internal Trade, *Draft National e-commerce Policy for Stakeholder Comments.*
44. "GDPR-loving EU says India's data localization unnecessary," *The Economic Times,* November 21, 2018, https://economictimes.indiatimes.com/tech/internet/gdpr-loving-eu-says-indias-data-localisation-unnecessary/articleshow/66725579.cms.
45. "Right to Privacy a Fundamental Right, Says Supreme Court in Unanimous Verdict," *The Wire,* August 24, 2017, https://thewire.in/law/supreme-court-aadhaar-right-to-privacy; "India: Watershed Year For Data Privacy Laws In India," Dhir and Dhir Associates, Monday website, accessed March 8, 2019, http://www.mondaq.com/india/x/711346/Data+Protection+Privacy/Watershed+Year+For+Data+Privacy+Laws+In+India; Anurag Bhaskar, "Key Highlights of Justice Chandrachud's Judgment in the Right to Privacy Case," *The Wire,* August 27, 2017, https://thewire.in/law/justice-chandrachud-judgment-right-to-privacy.
46. India's Department for Promotion of Industry and Internal Trade, *Draft National e-commerce Policy for Stakeholder Comments.*
47. Daniel Castro and Alan McQuinn, "Unlocking Encryption: Information Security and the Rule of Law" (Information Technology and Innovation Foundation, March 2016), http://www2.itif.org/2016-unlocking-encryption.pdf.
48. Ibid.
49. Reserve Bank of India, "Statement on Developmental and Regulatory Policies (April 5, 2018), press release, April 5, 2018.
50. Julia Fioretti, "EU looks to remove national barriers to data flows," *Reuters,* September 29, 2016, http://www.reuters.com/article/us-eu-data/eu-looks-to-remove-national-barriers-to-data-flows-idUSKCN11Z19Q.

51. "Requirements for Exemption to Store Electronic Accounting Records Abroad Will Be Abolished," Horten website, accessed November 9, 2017, http://en.horten.dk/News/2015/February/Requirement-for-exemption-to-store-electronic-accounting-records-abroad-will-be-abolished.

52. Nigel Cory and Robert Atkinson, "Financial Data Does Not Need or Deserve Special Treatment in Trade Agreements (Information Technology and Innovation Foundation, April, 2016), http://www2.itif.org/2016-financial-data-trade-deals.pdf; Rosalind Wiggins and Andrew Metrick, "The Lehman Brothers Bankruptcy: The Effect of Lehman's U.S. Broker Dealer" (Yale Program on Financial Stability Case Study 2014-3E-V1), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2588556; Administrative Office of the United States Courts, "Report Pursuant to Section 202(e) of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010" (Washington, D.C., July 2011); Lemieux, "Financial Records and Their Discontents"; "Lehman Brothers International (Europe) in Administration: Joint Administrators' Progress Report for the Period 15 September 2008 to 14 March 2009," PricewaterhouseCoopers, accessed April 4, 2016, http://www.pwc.co.uk/en_uk/uk/assets/pdf/lbie-progress-report-140409.pdf.

53. "Lehman Brothers International (Europe)) in Administration: Joint Administrators' Progress Report for the Period 15 September 2008 to 14 March 2009."

54. "Resolution Plans," Board of Governors of the Federal Reserve System, accessed April 4, 2016, https://www.federalreserve.gov/bankinforeg/resolution-plans.htm.

55. These "living wills" are required to provide a broad range of information relevant to resolution planning and implementation including, for example, detailed descriptions of organizational structures, credit exposures and cross-guarantees, and supporting data. The relevant section on IT and data states: "Management Information Systems; Software Licenses; Intellectual Property. Provide a detailed inventory and description of the key management information systems and applications, including systems and applications for risk management, accounting, and financial and regulatory reporting, used by the covered insured depository institution (CIDI) and its subsidiaries. Identify the legal owner or licensor of the systems identified above; describe the use and function of the system or application, and provide a listing of service level agreements and any software and systems licenses or associated intellectual property related thereto. Identify and discuss any disaster recovery or other backup plans. Identify common or shared facilities and systems, as well as personnel necessary to operate such facilities and systems. Describe the capabilities of the CIDI's processes and systems to collect, maintain, and report the information and other data underlying the resolution plan to management of the CIDI and, upon request, to the FDIC. Describe any deficiencies, gaps, or weaknesses in such capabilities and the actions the CIDI intends to take to promptly address such deficiencies, gaps, or weaknesses, and the time frame for implementing such actions."

56. Nigel Cory, "The Ten Worst Digital Protectionism and Innovation Mercantilist Policies of 2018" (Information Technology and Innovation Foundation, January 2019), https://itif.org/publications/2019/01/28/ten-worst-digital-protectionism-and-innovation-mercantilist-policies-2018.

57. World Trade Organization (WTO), "Work Programme on Electronic Commerce" (Geneva: WTO, WT/L/274, September 30, 1998), https://docs.wto.org/dol2fe/Pages/FE_Search/DDFDocuments/31348/T/WT/L/274.DOC.

58. Ludger Schuknecht and Rosa Pérez-Esteve, "A Quantitative Assessment of Electronic Commerce" (Geneva: Report for the World Trade Organization, September 1999), https://www.wto.org/english/res_e/reser_e/ae9901_e.htm.

59. Joe Kennedy, "The Myth of Data Monopoly: Why Antitrust Concerns About Data Are Overblown" (Information Technology and Innovation Foundation, March 2017), http://www2.itif.org/2017-data-competition.pdf; Robert Atkinson, "IP Protection in the Data Economy: Getting the Balance Right on 13 Critical Issues" (Information Technology and Innovation Foundation, January 2019), https://itif.org/publications/2019/01/22/ip-protection-data-economy-getting-balance-right-13-critical-issues.

60. For example, see Avanti Kumar, "Can Malaysia Really Become a Data Center Hub?" *MISAsia,* February 13, 2017, http://www.mis-asia.com/tech/data-centre/mdec-exclusive-can-malaysia-really-become-a-data-centre-hub/; "Indian Cloud Data Centres Will Make or Break Digital India," *FirstPost,* October 30, 2015, http://www.firstpost.com/business/sponsored-indian-cloud-data-centres-will-make-or-break-digital-india-2475598.html.

61. Michael S. Rosenwald, "Cloud Centers Bring High-Tech Flash but Not Many Jobs to Beaten-Down Towns," *The Washington Post*, November 24, 2011, http://www.washingtonpost.com/business/economy/cloud-centersbring-high-tech-flash-but-not-many-jobs-to-beaten-down-towns/2011/11/08/gIQAccTQtN_story.html; Henry Blodget, "The Country's Problem in a

Nutshell: Apple's Huge New Data Center in North Carolina Created Only 50 Jobs," *Business Insider*, November 28, 2011, http://www.businessinsider.com/apple-new-data-center-north-carolina-created-50-jobs-2011-11; Darrell Etherington, "Apple to Build a $2 Billion Data Command Center in Arizona," *TechCrunch*, February 2, 2015, https://techcrunch.com/2015/02/02/apple-to-build-a-2-billion-data-command-center-in-arizona/; Rich Miller, "The Economics of Data Center Staffing," *Data Center Knowledge*, January 18, 2008, http://www.datacenterknowledge.com/archives/2008/01/18/the-economics-of-data-center-staffing/; Alison DeNisco Rayome, "Why data centers fail to bring new jobs to small towns," *TechRepublic,* September 19, 2016, https://www.techrepublic.com/article/why-data-centers-fail-to-bring-new-jobs-to-small-towns/.

62. Grant Gross, "This Wave of Data Center Consolidation is Different from the First One," *Data Center Knowledge,* February 8, 2018, https://www.datacenterknowledge.com/manage/wave-data-center-consolidation-different-first-one.

63. John Lenio, "The Mystery Impact of Data Centers on Local Economies Revealed," *Area Development,* 2015, http://www.areadevelopment.com/data-centers/Data-Centers-Q1-2015/impact-of-data-center-development-locally-2262766.shtml.

64. Rich Miller, "The Economics of Data Center Staffing," *Data Center Knowledge,* January 18, 2008, https://www.datacenterknowledge.com/archives/2008/01/18/the-economics-of-data-center-staffing.

65. Dina Bass, "Microsoft Unveils Azure Sentinel Cloud Security Program," Data Center Knowledge, *February 28, 2019,* https://www.datacenterknowledge.com/microsoft/microsoft-unveils-azure-sentinel-cloud-security-program.

66. Emily Holbrook, "Facebook's New Utah Data Center Engineered to Be 'Incredibly Water Efficient,'" *Environmental Leader,* June 1, 2018, https://www.environmentalleader.com/2018/06/facebooks-new-utah-data-center-engineered-to-be-incredibly-water-efficient/.

67. Abhishek Raval, "India Becoming The New Battlefield For Data Center Providers," *Express Computer,* July 25, 2018, https://www.expresscomputer.in/magazine/india-becoming-the-new-battlefield-for-data-center-providers/17540/.

68. As part of the proxy variable for data regulations, the study uses part of the OECD's Product Market Regulation in services to create a proxy that comes close to matching the types of regulations that are used regarding data. The real policy regulations for the select countries are then added to this index to estimate the real costs. Matthias Bauer, Martina F. Ferracane, and Erik van der Marel, "Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization" (Centre for International Governance Innovation and Chatham House, May 2016), https://www.cigionline.org/sites/default/files/gcig_no30web_2.pdf.

69. The study uses U.S. Bureau of Economic input-output tables to identify which sectors are the heaviest users of a prescribed list of data-service sectors (such as software, Internet and broadcasting publishers, Internet service providers and web search portals, and data processing, hosting, and related services).

70. Overall, there is a small panel dataset for three years covering 21 goods and services sectors for 12 countries. The results of the regressions suggest that administrative regulatory barriers in sectors using data-processing services most intensively exhibit a dampening effect on TFP, while also exerting an upward pressure on prices in these sectors. A one standard-deviation change in the DRL variable would therefore decrease TFP on average by 3.9 percent. Similarly, for prices, a one standard-deviation change in the DRL would increase prices on average by 5.3 percent. Bauer, Ferracane, and van der Marel, "Tracing the Economic Impact of Regulations."

71. This second part uses the elasticities for TFP and the price index. It also augments the proxy of administrative barriers with actual or proposed barriers to data flows in the selected countries. This part identifies and weights (by severity of economic impact) the actual or proposed measures in these countries to derive a new index.

72. On a scale of 0–6: Russia is 4.82; China is 3.88; South Korea is 3.82; the European Union is 3.18; Indonesia is 2.42; India is 2.36; Vietnam is 2.19; and Brazil is 0.75.

73. The study uses the results from this augmented index back in the initial regression to calculate the actual TFP impact in the same set of data-intense downstream sectors in this set of countries. The results show that the services economy suffers the most from barriers to data flows, with TFP decreasing by 2 percent in the communication sector in South Korea, China, and the European Union. These downstream TFP estimates are then used in a computable general equilibrium model to estimate the impact on industrial output and trade volumes.

74. The study uses a computable general equilibrium model (CGE) called GTAP8. The effect on productivity is created using a so-called augmented product market-regulatory index for all regulatory barriers on data, including data localization, to calculate domestic price increases or total factor productivity losses. Matthias Bauer, Hosuk Lee-Makiyama, Erik can der Marel, Bert Verschelde, "The Costs of Data Localisation: Friendly Fire on Economic Recovery" (European Centre for International Political Economy, March 2014), http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf.

75. See Table 1 on page 4 for the full details for which countries have which policies. Bauer et al., "Costs of Data Localisation."

76. For example, the telecommunications sector is very data intensive (with 31 percent of its inputs being data related) and should be more heavily affected by regulation; similarly, data processing is 5 to 7 percent of the total inputs used by business/ICT and financial services. Intensities of data services for each sector are based on US input/output use tables from the US Bureau of Economic Analysis. Data on TFP and prices for each sector are taken from EU KLEMS databases.

77. Reena B. Gordon, Kati Suominen, *Going Global Promoting the Internationalization of Small and Mid-Size Enterprises in Latin America and the Caribbean* (Washington, D.C.: The Inter American Development Bank, 2014), https://publications.iadb.org/bitstream/handle/11319/6793/Going%20Global.pdf?sequence=1.

78. Feenstra, R. and H. L. Kee. 2004. "On the measurement of product variety in trade," Policy Research Working Paper Series 3213, Washington, DC: World Bank.

79. David Hummels and Georg Schaur, "Time as a Trade Barrier" (NBER Working Paper No. 17758, January 2012), https://www.nber.org/papers/w17758; David Hummels, Transportation Costs and International Trade in the Second Era of Globalization. *Journal of Economic Perspectives* 21, no. 3, 2007: 131–54. American Economic Association. Daniel Ikenson, "While Doha Sleeps: Securing Economic Growth through Trade Facilitation" (CATO Trade Policy Analysis no. 37, 2008), https://www.cato.org/publications/trade-policy-analysis/while-doha-sleeps-securing-economic-growth-through-trade-facilitation.

80. David Hummels and Georg Schaur, "Time as a Trade Barrier."

81. Andrew B. Bernard, J. Bradford Jensen, Stephen J. Redding, and Peter K. Schott, "The Empirics of Firm Heterogeneity and International Trade" (NBER Working Paper 17627, September 2012), https://www.annualreviews.org/doi/abs/10.1146/annurev-economics-080511-110928.

82. RV Anuradha and Trishna Menon, "India: India and the WTO's Trade Facilitation Agreement," Clarus Law Associates, Mondaq Website, accessed March 8, 2019, http://www.mondaq.com/india/x/741364/international+trade+investment/INDIA+AND+THE+WTOS+TRADE+FACILITATION+AGREEMENT.

83. Brett Danaher, Michael D. Smith, and Rahul Telang, "Copyright Enforcement in the Digital Age: Empirical Evidence and Policy Implication," *Communications of the ACM*, February 2017, Vol. 60 No. 2, Pages 68-75, https://cacm.acm.org/magazines/2017/2/212432-copyright-enforcement-in-the-digital-age/fulltext.

84. Nigel Cory, "How Website Blocking Is Curbing Digital Piracy Without "Breaking the Internet"" (Information Technology and Innovation Foundation, August, 2016), http://www2.itif.org/2016-website-blocking.pdf.

85. U.S. Department of Commerce, *Copyright Policy, Creativity, and Innovation in the Digital Economy* (Washington, D.C: Department of Commerce Internet Policy Taskforce, July 2013), https://www.uspto.gov/sites/default/files/news/publications/copyrightgreenpaper.pdf.

86. United States Intellectual Property Enforcement Coordinator (IPEC), *Annual Intellectual Property Report to Congress March 2018* (Washington, D.C.: IPEC), https://www.whitehouse.gov/wp-content/uploads/2017/11/2018Annual_IPEC_Report_to_Congress.pdf.

87. United States Intellectual Property Enforcement Coordinator (IPEC), *2013 Joint Strategic Plan on Intellectual Property Enforcement* (Washington, D.C.: IPEC, June 2013), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/IPEC/2013-us-ipec-joint-strategic-plan.pdf.

88. European Commission, "Face Sheet: Intellectual Property Rights Enforcement," European Commission website, November 29, 2017, accessed March 8, 2019, http://europa.eu/rapid/press-release_MEMO-17-4943_en.htm.

89. European Commission, "Statement by Vice-President Ansip at EU Blockathon 2018 on the Memorandum of Understanding on online advertising and intellectual property rights," European Commission website, June 25, 2018, https://ec.europa.eu/commission/commissioners/2014-2019/ansip/announcements/statement-vice-president-ansip-eu-blockathon-2018-memorandum-understanding-online-advertising-and_en.

90. Donuts and Motion Picture Association of America, "Donuts and the MPAA Establish New Partnership to Reduce Online Piracy," news release, February 9, 2016, https://www.mpaa.org/wp-content/uploads/2016/02/Donuts-and-MPAA-Establish-New-Partnership-2.9.16.pdf.

91. @ICANN_President, "Congrats Donuts & MPAA on collaborating to fight online piracy & showing the voluntary multistakeholder model works!," Twitter, February 9, 2016, https://twitter.com/icann_president/status/697135725297315840.

92. Daniel Castro and Nigel Cory, "Industry cooperation takes another step in fighting online piracy," *The Hill,* March 3, 2016, https://thehill.com/blogs/pundits-blog/technology/271587-industry-cooperation-takes-another-step-in-fighting-online.

93. Andrew Allemann, "11 domains affected by Donuts' "trusted notifier" deal with MPAA," *Domain Name Wire,* February 28, 2017, https://domainnamewire.com/2017/02/28/11-domains-affected-donuts-trusted-notifier-deal-mpaa/.

94. Radix and Motion Picture Association of America, "Radix and the MPAA Establish New Partnership to Reduce Online Piracy," news release, May 13, 2016, https://www.mpaa.org/wp-content/uploads/2016/05/Radix-and-the-MPAA-Establish-New-Partnership-to-Reduce-Online-Piracy.pdf.

95. "Operation Creative and IWL," City of London Police website, May 25, 2016, accessed March 8, 2019, https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/Pages/Operation-creative.aspx; "PIPCU secures £3.3m funding until 2019," *Trademarks and Brands Online,* August 22, 2017, https://www.trademarksandbrandsonline.com/news/pipcu-secures-3-3m-funding-until-2019-5061.

96. "PIPCU: the IP police," *Trademarks and Brands Online,* October 1, 2014, https://www.trademarksandbrandsonline.com/article/pipcu-the-ip-police.

97. "Operation Creative sees 64 per cent drop in UK advertising," City of London Police website, March 2, 2017, https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/pipcu-news/Pages/Operation-Creative-sees-64-per-cent-drop-in-UK-advertising-.aspx,

98. "Gambling adverts on illegal sites drop 87%: research," *Trademarks and Brands Online,* June 14, 2017, https://www.trademarksandbrandsonline.com/news/gambling-adverts-on-illegal-sites-drop-87-research-5015.

99. "Code of Conduct to promote lawful behavior on the Internet," multi-stakeholder declaration of intent, accessed March 8, 2019, https://kum.dk/fileadmin/KUM/Documents/Nyheder%20og%20Presse/Pressemeddelelser/2015/Code_of_Conduct_-_Engelsk_version.pdf; "Codex – promoting legitimate online marketing," website accessed March 8, 2019, http://adkodex.com/codex/.

100. European Union Intellectual Property Office, *Digital Advertising on Suspected Infringing Websites* (Brussels: Office for Harmonization in the Internal Market, European Union Intellectual Property Office, January, 2016), https://euipo.europa.eu/ohimportal/documents/11370/80606/Digital+Advertising+on+Suspected+Infringing+Websites.

101. Ari Juliano Gema, "Intellectual property rights: Indonesia can win the war on online piracy," *The Jakarta Post,* May 3, 2018, https://www.thejakartapost.com/academia/2018/05/03/intellectual-property-rights-indonesia-can-win-the-war-on-online-piracy.html; Masriwanie Muhamading, "Malaysia launches Infringing Website List initiative to combat digital piracy," *New Strait Times,* October 10, 2017, https://www.nst.com.my/news/nation/2017/10/289556/malaysia-launches-infringing-website-list-initiative-combat-digital; Lauly Li, "MOU signed to cut ads on piracy sites," *Taipei Times,* September 5, 2017, http://www.taipeitimes.com/News/biz/archives/2017/09/05/2003677797.

102. "Infringing Website List enlists 50 HK brands to cut pirate ad revenue," *Marketing Interactive,* October 4, 2017, https://www.marketing-interactive.com/infringing-website-list-enlists-50-hk-brands-to-cut-pirate-ad-revenue/.

103. European Union-Japan Economic Partnership Agreement., article 8.73; United States-Mexico-Canada Agreement, 19.16.2; Comprehensive and Progressive Agreement for Trans-Pacific Partnership article 14.17.

104. See: Russia 2 Russian Federal Security Services can demand tech firms hand over encryption keys. Failure to comply lead to their services being blocked in Russia in accordance with the 2016 Federal Law No. 374 on Amending the Federal Law on Counterterrorism and Select Legislative Acts of the Russian Federation Concerning the Creation of Additional Measures Aimed at Countering Terrorism and Protecting Public Safety. Peter Roudik, "Russia: New Electronic Surveillance Rules," Library of Congress website, July 18, 2016, https://www.loc.gov/law/foreign-news/article/russia-new-electronic-surveillance-rules/.

105. WTO, TRIPS, article 39

106. *Defend Trade Secrets Act of 2016*, 114th Congress, https://www.congress.gov/bill/114th-congress/senate-bill/1890/text.

107. "Trade Secrets," European Commission website, accessed August 7, 2018, http://ec.europa.eu/growth/industry/intellectual-property/trade-secrets_en.

108. "Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA)," Office Journal of the European Union website, accessed August 7, 2018, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF.