

# Data is disruptive: How data sovereignty is challenging data governance

BY SUSAN ARIEL AARONSON



# Contents

<b>INTRODUCTION</b>	3
<b>WHAT IS DATA, DATA-SHARING, AND REUSE?</b>	7
<b>DATA-ECONOMY BUSINESS MODELS</b>	10
The future currency: our personal data	11
<b>EMERGING INSIGHTS INTO DATA GOVERNANCE</b>	12
<b>GOVERNING DATA THROUGH TRADE AGREEMENTS</b>	14
<b>EXAMPLES OF DATA SOVEREIGNTY: INDIA, THE US, AND CHINA</b>	17
India: human rights and government authority	17
The United States: protecting data for national security	18
China: national security over commerce	18
<b>CONCLUSION</b>	20
<b>RESEARCHER BIO: SUSAN ARIEL AARONSON</b>	21
<b>ENDNOTES</b>	22

# Introduction

Chinese and Indian officials do not often agree on how to see the world.<sup>1</sup> Yet their views converge on one issue: Government officials must control the flow of data from users to firms and from firms to users – at home and abroad.

According to *The Wall Street Journal*, China's President Xi Jinping allegedly commented during a private meeting that, "Whoever controls data will have the initiative."<sup>2</sup> As China's firms become globally competitive in data-driven sectors, Beijing has wielded more and more authority over public and private troves of data.

India has similar aspirations. In 2019, Piyush Goyal, who was then Minister of Commerce and Industry, underlined the government's view that data is a sovereign asset.<sup>4</sup> That same year, Ravi Shankar Prasad, who served as Minister for Communications, Electronics and Information Technology, and Law and Justice, described India's control of the country's data as "non-negotiable."<sup>5</sup>

For China and India, the right to control the collection, ownership, and application of citizens' data should rest with national policymakers.

For China and India, the right to control the collection, ownership, and application of citizens' data – heretofore referred to as **data sovereignty** – should rest with national policymakers.

They are not alone. Tasked with protecting and enhancing Europe's digital sovereignty, Thierry Breton, Internal Market Commissioner for the European Union (EU), works to ensure that European data is "used for European companies...to create value in Europe."<sup>6</sup>

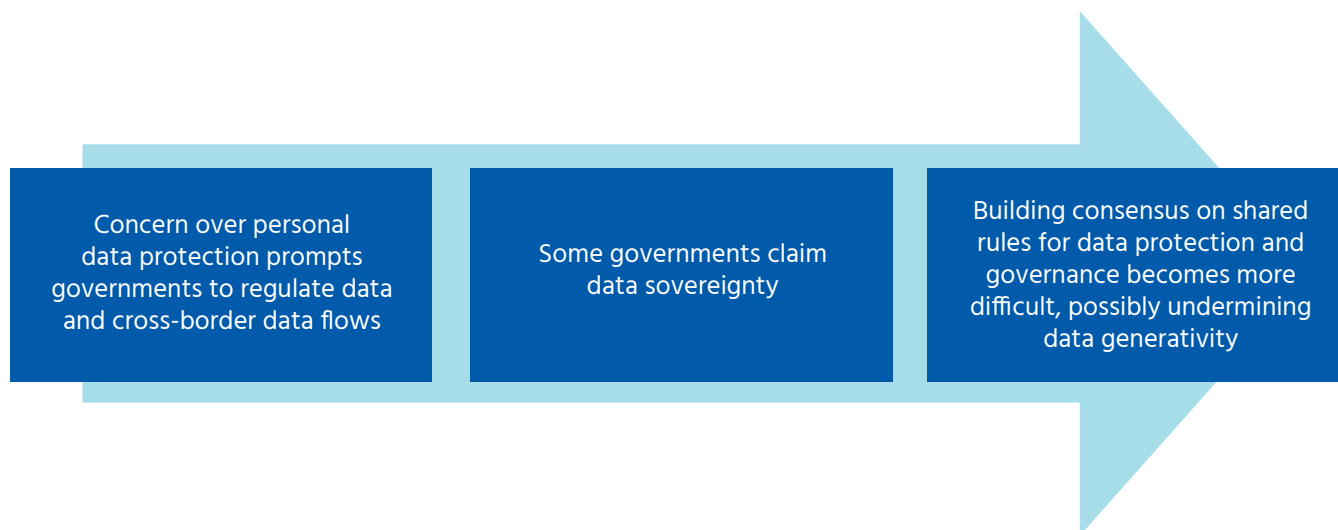
In Canada, officials have warned that the country, "cannot ensure full sovereignty over its data when it stores data in the cloud. Sensitive (government data) could be subject to foreign laws and be disclosed to another government."<sup>7</sup> Canada's best options, concluded policymakers, are to limit categories of data stored in the cloud, encrypt the data, and use contracts to ensure only Canadians could access sensitive data.<sup>8</sup>

Why are these governments promoting a vision of data sovereignty? Philosopher Luciano Floridi has a theory, and it centers around power. In 2020, Floridi described the struggle for digital sovereignty is between companies and states:

"Companies design, produce, sell, and maintain the digital ecosystem, and states are dependent on these firms. But states have the power to regulate the digital space."<sup>9</sup>

Many recognize that failing to protect personal data and online privacy could create a vicious cycle.

But firms and governments are not the only factors that policymakers consider for the governing of data. Policymakers claim to act on behalf of users who need to trust that their data is safe and secure and that their rights are protected. Many recognize that failing to protect personal data and online privacy could create a vicious cycle. Over time, users could have less autonomy and feel less comfortable stating their opinions online. In turn, that can undermine trust, democracy, and collective self-determination.<sup>10</sup>

**Figure 1 – Data is disruptive**

Some policymakers argue that the best way to protect citizens' data while encouraging data-driven development is to ensure that data resides in local servers, under domestically determined rules, and the control of national authorities.

Indeed, some governments use personal data protection and data sovereignty as a means to control or even hoard data.

Indeed, some governments use personal data protection and data sovereignty as a means to control or even hoard data. Since 2019, India, the world's most populous democracy, has debated strict rules governing personal data collection and monetization by firms. Yet India exempts the government from such rules. China, the world's most populous nation, has approved stringent laws requiring firms to protect personal data. Here too public sector entities are generally exempted from the rules. Why are policymakers from these countries able to exempt the public sector from protecting personal data? These nations have large populations and growing markets which translate into leverage over other countries and data-driven firms.

Chinese and Indian officials may believe that command over vast quantities of data provides competitive advantage in the data-driven economy. They understand that successful Artificial Intelligence (AI) systems require large amounts of data.

Their vision of data control as a means of protecting personal data is disruptive.

First, the model makes it more difficult to build a global consensus on shared rules for governing cross-border data flows, a key element of global data governance.

Whether held by the public or private sector, large inventories of data are most useful when they are used, shared, and crossed with other sets of data.

The vision may also be inaccurate. When countries insist their data is "sovereign", they risk the generativity of data as well as its larger public benefits. Whether held by the public or private sector, large inventories of data are most useful when they are used, shared, and crossed with other sets of data.<sup>11</sup> Policymakers should not control data in ways that limit its utility for society at large.<sup>12</sup>

### **A road not yet traveled**

As data has become essential to economic growth, data governance has become critical to modern governance. Yet many officials are just learning to navigate this new component of governance.

Most governments have adopted national rules to govern three types of data: public, personal, and proprietary data.

Most governments have adopted national rules to govern three types of data: public, personal, and proprietary data. However, there is no explicit international agreement governing cross-border data flows. Because cross-border data flows underpin the internet and the global economy, both domestic and international rules are important.

Since 2003, trade diplomats have negotiated many regional and bilateral agreements that cover personal, proprietary, and often public data. Often, the agreements include provisions that make the free flow of data across borders the default.

However, the deals also allow “exceptions.” Presented in terms of legitimate public policy objectives,<sup>13</sup> these exceptions can be very broad. Indeed, they enable nations to adopt a wide range of strategies that justify taking greater control of data in the national interest.

Moreover, the agreements do not incentivize shared interoperable approaches to data governance. Thus, without intentionally doing so, regional and bilateral trade agreements may actually facilitate attempts to assert data sovereignty.

Since 2019, the World Trade Organization (WTO) has also been trying to negotiate rules governing cross-border data flows.

Since 2019, the World Trade Organization (WTO) has also been trying to negotiate rules governing cross-border data flows. However, although 86 WTO members are participating in the talks, 78 developing economies choose to not participate. Fearing that data will be disruptive to their development, these nations are not ready to develop shared rules.

WTO members have found some areas of agreement. After a year of negotiations, they have finalized texts on spam, electronic signatures, and electronic authorization. They believe that an agreement can also be reached on rules for governing open government data and online consumer protection. What remains under negotiation is the language for governing cross-border data flows and rules for new services built on data, such as AI.<sup>14</sup>

This paper is an overview of the complicated issue of data governance and trade. By examining both national and international components of data governance and relating them to growing calls for data or digital sovereignty, the paper outlines the evolving challenges that can affect digital trade.

The overview has five parts. The first section defines data and describes how data analytics fuels economic growth. Then I discuss data sharing and reuse, platform business models, and the role of personal data in the data-driven economy. The overview then focuses on the state of national and international data governance and the potential role of trade agreements in facilitating greater government control of data. The fourth section describes how the US, China, and India attempt to wield more control of data in the domestic and international arena. I then develop conclusions and make some recommendations for policymakers.

In Figure 2 below, key terms are delineated to help the reader follow the argument. These definitions were provided by the Organization for Economic Development and Cooperation (OECD).

**Figure 2 – Definitions of data governance**

<b>Data</b>	Information that can be expressed as zeros and ones and hence can be utilized by researchers in digital processes
<b>Data governance</b>	Principles, policies, standards, laws, regulations, and agreements designed to control, manage, share, protect, and extract value from various types of data. This overview focuses on data governance by government officials
<b>Digital trade</b>	Digitally enabled transactions of trade in goods and services that can either be digitally or physically delivered, and that involve consumers, firms, and governments willing to use domestic regulations (data governance) or digital trade policies to ensure greater control of various types of data
<b>Personal data</b>	Any information relating to an identified or identifiable individual (data subject)
<b>Non-personal data</b>	Electronic data that does not contain any information that can be used to identify a natural person. It can include anonymized personal data or non-personal data such as corporate tax receipts
<b>Big data</b>	Large data sets of either personal or non-personal data. Characterized by such a high volume, value, velocity, and variety to require specific technology and analytical methods for its transformation

Source: OECD

# What is data, data-sharing, and reuse?

Data is ubiquitous. It comes in many formats, from structured, numeric data in traditional databases, to unstructured text documents, emails, videos, or financial transactions. Data has become essential for producing almost everything, from soybeans to social networks.

Historically, firms, researchers, and policymakers used data to improve the efficiency and quality of goods and services. Today, firms collect large pools of personal data to provide new services, such as the social network Strava or Covid-19 travel passports.

Despite the importance of data, researchers have long struggled to illuminate the role of big data in the economy. Here are some of the challenges in categorizing data.

Data performs many different functions: it can be a product, consumption, or act as an intermediary. Data effects the economy at the individual, household, firm, national, and international levels.

First, data performs many different functions: it can be a product, consumption, or act as an intermediary. Data effects the economy at the individual, household, firm, national, and international levels.<sup>15</sup>

Second, while the internet is built on cross-border data flows that we describe as traded, many of those data flows are not associated with a financial transaction. Hence it is hard to describe such flows as “traded.”<sup>16</sup>

Third, trade in the same set of data is fluid and frequent. Location can be hard to determine. As a result, we do not know when data is exported or imported.

Fourth, firms have developed proprietary business models for valuing data. These models are difficult to compare across sectors and at the national level. As a result, analysts struggle to measure data inputs in the production process.

Finally, due to the challenges of measuring data and data flows, the value of digital trade is also difficult to determine with accuracy.

Although we can't state with confidence the exact value of data, we can say that data drives the modern economy.

According to the US Department of Commerce, exports of potential digitally enabled services reached US\$499 billion, comprising more than half of US services exports.

According to the US Department of Commerce, US exports of information and communication technology (ICT) goods and services in 2018 amounted to an estimated US\$148 billion and US\$80 billion, respectively. In addition, exports of potential digitally enabled services reached US\$499 billion, comprising more than half of US services exports.<sup>17</sup>

The UK Trade Policy Observatory estimates that in 2019, international e-commerce represented a staggering US\$3.6 trillion, to which digitally delivered services would add another US\$ 2 trillion. In sum, digital trade then was likely worth US\$5.5 to US\$6 trillion, or almost 25% of total world exports.<sup>18</sup>

Without robust statistics, analysts often rely on analogies to convey how data is forcing change to the economy and the polity. Some describe data as a resource.



Others view it as an asset or a form of capital. Some view personal data as a form of undercompensated labor; hence users must organize to control and receive revenue from their data.<sup>19</sup> Others yet – for example, proponents in the UK government – argue that data is a form of infrastructure that governments should provide and manage on behalf of their citizens.<sup>20</sup>

These analogies are colorful, but they do not convey the full picture of data's role in the economy. Without good statistics and broad understanding, policymakers around the world struggle to develop effective and well-targeted policies for the digital era.<sup>21</sup>

We do know that data behaves differently from other economic inputs, such as land or capital. First, data derives value not from the data itself, but from the actions of researchers, firms, and governments to create value from the data. Moreover, both personal or non-personal data can be used and reused without risking its depletion.<sup>22</sup>

Data is unusual in another way. Researchers and firms can create value by sharing data. They can also create value by denying others the ability to use the same set of data. When states or firms restrict access to data – whether through hoarding, regulations, or intellectual property (IP) rules – they can diminish the potential for economic growth, productivity, and innovation.<sup>23</sup>

Sharing data is critical to promoting scientific progress and encouraging a culture of openness and accountability. When data is simply stored or hoarded, it cannot be used to create new products or services, or as input for analyzing complex problems.<sup>24</sup>

Finally, all governments do not have equal influence and expertise in governing data. Some countries have greater influence over data and data-driven firms because some of those firms were home-grown and often relied on taxpayer-supported innovations, such as the internet and AI.

Both the US and China have years of experience dealing with the tech giants, and to some degree these firms cannot afford to alienate home country users and policymakers. Other nations and trade blocs such as the EU have influence due to their size or because they are growth markets for the data-driven services they are seeking to regulate.

Small countries – even the most tech savvy such as Canada – may find themselves lacking influence over the big tech firms. While their small market size plays a role, they may also lack information about how the firms operate.<sup>25</sup>

### Figure 3 – Platform varieties

Type of platform	Example
Transaction platforms	Amazon, Alibaba, Airbnb, Uber, Baidu, eBay
Technology platforms	Microsoft 360, Google Play, Apple Appstore
Connectivity platforms	Amazon Alexa, Samsung SmartThings

Without good statistics and broad understanding, policymakers around the world struggle to develop effective and well-targeted policies for the digital era.

Sharing data is critical to promoting scientific progress and encouraging a culture of openness and accountability.



Many developing countries have even greater gaps in data governance expertise. According to the World Bank, lower-income countries lack “the infrastructure and skills to capture data and turn them into value.”<sup>26</sup> Many lower income countries, the Bank added, “lack the institutional and regulatory frameworks to create trust in data systems, and the scale and agency to participate equitably in global data markets and their governance.”<sup>27</sup>

Not surprisingly, the OECD has warned that the data-driven economy will shift the power balance in the economy.

Not surprisingly, the OECD has warned that the data-driven economy will shift the power balance in the economy in three ways. Power will shift away from individuals to organizations, from traditional businesses to data-driven businesses, and from governments to data-driven businesses. The OECD argues that these firms may obtain more knowledge about citizens than governments. These shifts could exacerbate existing inequalities and lead to a new ‘data’ divide that, if not addressed, could undermine social cohesion and economic resilience.<sup>28</sup>

One way to address this divide is to gain a deeper understanding of how firms use personal data and use those insights to guide data governance.

# Data-economy business models

While many companies have large reservoirs of data, some 25 internet companies control vast amounts of this data.

While many companies have large reservoirs of data, some 25 internet companies control vast amounts of this data. These companies have extremely high valuations – an expression of what markets think a company’s tangible and intangible assets are worth.<sup>29</sup> Although they are global, their headquarters are mainly in the US or China.<sup>30</sup>

Many of these companies do not just analyze data; they act as both intermediaries and infrastructure for data. Scholars refer to them as “**platforms**,” or venues where market actors can exchange ideas, goods, and services. Such platforms can lower transaction costs and stimulate better use of underutilized resources. However, their market power enables them to buy up competitors, and subsequently reduce innovation and workers’ bargaining power.<sup>31</sup>

There are several types of platforms. Transaction platforms such as Amazon, Alibaba, Airbnb, Uber, and Baidu match supply with demand. Technology platforms such as Microsoft’s software platform and the app stores of Google and Apple provide an infrastructure upon which others can build. Other platforms such as Amazon’s Alexa and Samsung SmartThings connect us to our devices.<sup>32</sup>

The platforms take advantage of what economists call network effects: the more users utilize the platform, the more valuable the platform becomes to users and investors. The more valuable the platform, the greater its ability to acquire, control, and analyze data. Users often become reluctant to leave platforms because they flock to sites where they can find people with whom they want to connect.<sup>33</sup>

The platform companies also benefit from “information asymmetries.” When these firms sell data, they accumulate more knowledge about market factors, such as price, cost, supply, and demand. Their voluminous data on data and on the markets for data gives them a comparative advantage. Markets for data are opaque; researchers are typically not versed in supply and demand, prices, and quality.<sup>34</sup> This opacity enables firms to take more data than they need and hoard data. As a result, users receive “too little privacy”.<sup>35</sup>

The opacity of data markets may also encourage firms to adopt or continue business practices that are harmful to society.

The opacity of data markets may also encourage firms to adopt or continue business practices that are harmful to society.

Many platforms use the so-called ‘freemium’ model. This model, which depends on advertisements for revenues and profits, offers free services, but users must first provide personal data, such as their interests or search history. After aggregating the data, the firms employ it to provide users with both tailored advertising and free content.<sup>36</sup> Some critics accuse many of the platforms of feeding divisive content to increase users’ time on the platform. More time on the platform encourages more advertisers and ever more data collection.<sup>37</sup>

In the data-driven economy, data begets both scale and other rewards. As they grow, the platforms amass significant computing power, which they use to transform data into new value-added data products. The new products and

services generate even more data and perpetuate the firms' market power. Because data-driven firms make large capital investments to analyze this data, they gain ever more advantage in attracting expertise and funding.

Secondly, the platforms tend to use their own intellectual property (IP), such as algorithms, to analyze data. As a result, they control the results of the analysis and the reuse of the analyzed datasets.<sup>38</sup> To fuel growth, firms may learn to rely on rents rather than innovation.<sup>39</sup>

Over time, rather than using or sharing data, entities may choose to merely store data.

Researchers and rights advocates highlight that firms often misuse personal data to manipulate users in ways that can threaten our autonomy, individual rights, and governance systems.

As noted earlier, the platforms' business models can also bring substantial costs to democratic stability and human rights. Researchers and rights advocates highlight that firms often misuse personal data to manipulate users in ways that can threaten our autonomy, individual rights, and governance systems.<sup>40</sup>

The problem has become so acute that government agencies in the US, home to many of the giant firms, have expressed concern. The US National Intelligence Council has cautioned that:

"Privacy and anonymity may effectively disappear by choice or government mandate, as all aspects of personal and professional lives are tracked by global networks."<sup>41</sup>

### The future currency: our personal data

Many large firms hold huge troves of historical and current personal data, which can be hacked, stolen, or manipulated.

For many years, the bulk of personal data was held by individuals and the public sectors of their respective countries. Data was once an item that researchers had to request to store and analyze.

Typically, users do not know for how long the firms will hold the data, the extent of data already in the firms' possession and how the data is used and for what purposes.

Today, our daily activities are sources of data collection.<sup>42</sup> The firms that provide us with 'free services' collect our data for categorization and analysis. Most people do not understand that they are the product of the 'free' services. Indeed, they have little information overall about the data collection. Typically, users do not know for how long the firms will hold the data, the extent of data already in the firms' possession (although they can learn this from individual firms), and how the data is used and for what purposes. Moreover, their data may be stored in one country, analyzed in another, and sold to advertisers globally.

Hence, users should be advocates for clear rules governing cross-border data flows that include interoperable rather than national approaches to protecting personal data.

# Emerging insights into data governance

Although data governance systems are in their infancy, some insights are emerging about how nations govern data. Our team at the Digital Trade and Data Governance Hub at George Washington University recently examined 52 countries in depth. The team examined governance of three types of data – personal, public, and proprietary – and found that most countries had laws or regulations governing these different types of data. We did not assess the effectiveness of the laws or regulations.

Not surprisingly, almost every country in the study had adopted laws and regulations governing personal data. The United Arab Emirates was the only country that had not yet adopted such a law. Relevant to this overview, 64 percent of the cases took significant further steps, by enacting laws that govern public sector and private sector use of personal data. The countries also required that users be able to provide informed consent for the use of their personal data. Furthermore, they sought the establishment of an agency to enforce the law, and rules governing third party transfer or sale of personal data.

The EU's approach to personal data protection is influential globally, yet it could be viewed as a form of regulatory bullying.

The EU's approach to personal data protection is influential globally, yet it could be viewed as a form of regulatory bullying. The EU won't allow countries to exchange personal data of EU citizens unless these countries are rated by an EU committee as adequate. Since the EU is the main trading partner for many nations, many nations are eager to become adequate. However, the EU has deemed only 15 countries as having an adequate level of personal data protection for data to flow freely.<sup>43</sup>

Over 80 percent of the studied countries had a law requiring that public data – data collected, utilized, analyzed, and funded by the government – should be open and available online for anyone to utilize, with limited exceptions for privacy and national security. Yet many nations, including low-income countries, are still figuring out how to govern public data and make it useful to their constituents, whether for research or business purposes.

Intellectual property protection is a key element of data protection, and many firms use trade secrets to protect their algorithms and modes of data analysis.

Intellectual property protection is a key element of data protection, and many firms use trade secrets to protect their algorithms and modes of data analysis. Unsurprisingly, 76 percent of the studied countries had enacted a trade secrets law, and 80 percent participated in an international trade agreement with trade secrets provisions. However, 47 percent of nations with a trade secret law did not allow firms using data analytics to explicitly control the data, using a mechanism protected under trade secrets.

In general, countries agreed to aspirational rather than binding language in their bilateral and regional trade agreements. Some 78 percent of the case studies are involved in agreements with aspirational language on cyber-security.<sup>44</sup> Meanwhile, 71 percent are parties to agreements with aspirational language stating the importance of interoperability of personal data protection. Because the binding language requires nations to enforce their own laws, aspirational language provides no means of fostering interoperability.

Data mixing is important because it is likely to facilitate greater insights into complex problems such as global warming.

We found evidence of important new trends in data governance related to data mixing and data sharing. As an example, several governments recognize that they will need to create new regulations governing which entities should control the mixed data. This is why some governments restrict the use of trade secrets with data sets and data analytics. Such data mixing is important because it is likely to facilitate greater insights into complex problems such as global warming. We also found that a growing number of governments recognize that large troves of personal data can lead to collective group harms. Hence they are regulating not just individual but group harms.

While policymakers emulate what they may see as effective data governance, so far they are struggling to find common ground on shared international data governance.

# Governing data through trade agreements

Since the first e-commerce agreement signed by Australia and Singapore in 2003, some 72 jurisdictions have signed regional trade agreements – and most recent agreements include provisions on cross-border data flows.<sup>45</sup> Hence policymakers have some experience in using trade to govern data flows, including personal data. Yet their efforts to control personal data at the national level make it more challenging to achieve consensus at the international level.

Many of the countries signing such agreements have their own templates for digital trade. There seems to be consensus, however, about what these agreements should say about how to govern data flowing between countries.

Every agreement permits signatories to breach the free flow rules for domestic policy purposes that are deemed necessary and legitimate.

First, while signatories agree that data should flow freely, exceptions apply. Every agreement permits signatories to breach the free flow rules for domestic policy purposes that are deemed necessary and legitimate. These exceptions include protecting national security, social stability, public health, and/or privacy.

Additionally, EU agreements such as the EU/UK Trade and Cooperation Agreement state that while non-personal data can flow freely across borders, personal data of Europeans can only flow to nations that have an adequate or equivalent data protection regime. But as mentioned earlier, few nations are deemed “adequate.”

However, there are few shared norms and definitions regarding how nations should behave when rules encouraging cross-border data flows conflict with the need to restrict such flows to protect privacy or social stability, as an example.

Without the further development of mechanisms to bridge regulatory differences between countries, the exceptions risk becoming the rule.

Signatories are supposed to use the exceptions only when necessary and in a non-discriminatory manner. Yet they can easily use exceptions to take greater control over data. The US used the national security exception to justify its review of foreign firms that seek to acquire data-rich companies such as Grindr. Canada is moving in a similar direction.<sup>46</sup> China justifies its Great Firewall in the name of protecting social stability. Nations such as India or Haiti that shut down the internet could also use the exceptions to defend such shutdowns or to justify protection from cyber-thefts, disinformation, cyberattacks on critical infrastructure. Without the further development of mechanisms to bridge regulatory differences between countries, the exceptions risk becoming the rule.<sup>47</sup>

Secondly, signatories agreed to ban two key practices. First, the practice of data localization, which requires that data must be stored and/or analyzed locally. The second practice involves performance requirements; for example, mandating a business to build a factory or invest in a firm to operate in a country. But signatories have not addressed other practices that have even broader effects on market access, such as internet shutdowns or disinformation.<sup>48</sup>

Thirdly, almost every digital trade agreement has provisions relating to personal data protection, spam, and consumer protection. These provisions generally require signatories to enforce their own laws. But the giant data firms are global and if nations need to challenge their practices, they may need to work together to foster internationally accepted or interoperable strategies.

Some countries recognize the dangers of failing to promote interoperable governance rules.

Some countries recognize the dangers of failing to promote interoperable governance rules. In their groundbreaking Digital Economy Agreement, Singapore and Australia agreed to collaborate on standards and work towards regulatory coherence.<sup>49</sup> The partners recognized the risk that:

“National efforts may create barriers that impede trade. It could lead to disparate technologies and platforms that are unconnected and unable to facilitate a seamless flow of cross-border trade.”<sup>50</sup>

Others are following suit. In 2021, the G7 countries – the world’s seven largest economies – stated that, “Differences in domestic approaches can impact cross-border data flows, creating uncertainty.” G7 officials are now working to identify how to achieve good regulatory practices and cooperation between nations.<sup>51</sup>

The recent digital trade agreements and how they address the free flow of data, the exceptions, and regulations, are compared in figure 4 below.

**Figure 4 – How the most recent digital trade agreements regulate cross-border data flows**

Provision	USMCA	EU-UK TCA	CPTPP	DEPA	AU/SG DEA	US-Japan DTA
Language explicitly encouraging cross-border data flows	<a href="#">Yes</a>	<a href="#">Yes</a>	<a href="#">Yes</a>	<a href="#">Yes</a>	<a href="#">Yes</a>	<a href="#">Yes</a>
GAT/GATS exceptions	Yes	Yes	Yes	Yes	Yes	Yes
Bans on performance requirements such as sharing source code and/or algorithms	<a href="#">Yes</a>	<a href="#">Yes, source code only</a>	<a href="#">Yes, source code only</a>	<a href="#">Yes</a>	<a href="#">Yes</a>	<a href="#">Yes</a>
Ban on data localization	<a href="#">Yes</a>	<a href="#">Yes</a>	<a href="#">Yes</a>	<a href="#">Yes</a>	<a href="#">Yes</a>	<a href="#">Yes</a>
Enforce your own laws for spam, consumer welfare, personal data protection	Yes	Yes	Yes	<a href="#">Yes</a>	<a href="#">Yes</a>	<a href="#">Yes</a>

Table by Andrew Kraskewicz with S. Aaronson

Some countries are adopting policies that facilitate policymakers’ ability to take greater control of data. The aforementioned study by the Digital Trade and Data Governance Hub found that almost every one of our 52 case studies had adopted national strategies to facilitate AI, smart manufacturing or other data-driven technologies. Some of the national plans require data to be stored or processed in local servers, making it harder for data to flow across borders. Another country might ban foreign ownership of certain data-based services. Still another might tax firms that profit from the personal data of its citizens but have no physical establishment in that country.

These strategies can distort trade and lead to uncertainty among firms and individuals. As an example, the US and the EU have spent months struggling to reconcile their different strategies for personal data protection.<sup>52</sup> Until the two



Some developing countries refuse to negotiate international data governance until they receive capacity building assistance or special and differential treatment to nurture their own data-driven economy.

trade giants find common ground on a mutually accepted approach, firms will not know what is required of them. Until they know the specifics, these firms may be less willing to invest in data protection strategies.

Finally, some developing countries refuse to negotiate international data governance until they receive capacity building assistance or special and differential treatment to nurture their own data-driven economy. South Africa and India provided the following explanation:

“Digitalization affects different countries in different ways and individual governments require policy space to regulate the digital economy” to meet legitimate public policy objectives. If developing countries are to make progress, they need to implement “active industrial policies to get some benefits of e-commerce.”<sup>53</sup>

Indeed, developing countries faced a tough choice in deciding whether to participate in these talks.

On one hand, many developing countries are not well-placed to profit from data-driven development. Although personal data is plentiful among their populace, fewer of their citizens have the skills to use this data to create new services. These countries will have to decide whether it makes sense to invest in transitioning towards a data driven economy which could yield few jobs and where they are unlikely to achieve economic advantage.<sup>54</sup>

On the other hand, the UN Conference for Trade and Development (UNCTAD) argues that these states will need to import data analytics to ensure that their other goods and services remain competitive.<sup>55</sup> By participating in the talks, developing countries might be able to negotiate better terms of trade for these exports as well as for their citizens’ data.

# Examples of data sovereignty: India, the US, and China

Trade policymakers rely on broad rationales – including protecting human rights, maintaining social stability, or protecting national security – to justify exercising more control of personal data.

While governments of developing countries argue that authority over data is important for economic development, middle and high-income countries also want special dispensation.

Generally, trade policymakers rely on broad rationales – including protecting human rights, maintaining social stability, or protecting national security – to justify exercising more control of personal data.

The paper has outlined the EU's requirement for firms or bodies to implement and maintain "reasonable security" procedures and protections to safeguard the data of EU citizens and residents.<sup>56</sup>

The following are other examples of assertions of data sovereignty.

## India: human rights and government authority

India uses social stability as well as human rights rationales to justify its efforts to exercise authority over both personal and non-personal data. Consider, for example, the government's increasing concern about the spread of rumors and social unrest on social media platforms such as WhatsApp, TikTok, and Twitter. In May 2021, Ravi Shankar Prasad, then India's Minister for Communications, IT, Law, and Justice, ordered social media companies to acknowledge takedown requests of unlawful, misleading, and violent content within 24 hours. To comply, most platforms, which are generally foreign owned, will have to significantly alter their operating model. The new law also requires the firms to keep tabs on individuals who use the platforms to send messages online. In May 2021, WhatsApp filed a lawsuit protesting the new laws.<sup>57</sup>

India's officials have long argued that government control over data protects citizens from harm. In 2011, the Indian Parliament amended the Information Technology Act ("IT Act") to include new provisions which allow individuals to request compensation for the improper disclosure of personal information. The government subsequently issued new rules for businesses that apply to the collection and disclosure of sensitive personal data. There is an important caveat, however: the government itself is not subject to these rules.<sup>58</sup>

More than half a billion Indians subscribed to the internet in 2018, a connectivity level second only to China.

The government's actions are significant because India is an enormous and rapidly growing market in the digital economy. More than half a billion Indians subscribed to the internet in 2018, a connectivity level second only to China.<sup>59</sup> While that is a large number compared to the rest of the world, it accounts for only 40 percent of India's population. Given its large market potential, India has leverage over the giant data companies. Most other developing countries lack this leverage.<sup>60</sup>

In recent years, India has been considering a draft bill on data protection. Like many other data protection laws, the bill's current iteration prescribes compliance requirements for all forms of personal data, broadens the rights given to individuals, introduces a central regulator for data protection, and institutes data localization requirements for certain forms of sensitive data. The bill also applies

extra territorially to non-Indian organizations and imposes hefty financial penalties in cases of non-compliance.<sup>61</sup> Again, the government is exempt from adopting these safeguards.<sup>62</sup>

### The United States: protecting data for national security

The US has long been the leading proponent of free flow of data across borders. However, increasingly the US is also using national security as a rationale to control data.

The Foreign Investment Risk Review Modernization Act (FIRRMA), which required the Treasury Department to review foreign investment in technologies essential to national security, including security-related infrastructure and other areas.

In 2018, Congress passed the Foreign Investment Risk Review Modernization Act (FIRRMA), which required the Treasury Department to review foreign investment in technologies essential to national security, including security-related infrastructure and other areas.<sup>63</sup>

Then, in 2019, former President Donald Trump issued an Executive Order, which described foreign adversarial investment in information technologies or services as, “an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.” A ban was subsequently issued on:

“Any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service (transaction) by any person...subject to the jurisdiction of the United States.”<sup>64</sup>

To determine if a foreign firm could exploit data in a manner that threatens US national security, the Treasury then began to review transactions involving the sensitive personal data of US citizens. These orders led to bans on platforms WeChat and TikTok, which originated from China. The orders took place despite lack of direct evidence that the firms share data with China, or of the threat to national security from misuse of users’ data.<sup>65</sup>

In June 2021, the Biden Administration rescinded these bans and promised a new approach to determine whether foreign investment in data-rich firms threatened users and national security.<sup>66</sup> Meanwhile, a key Senator suggested two new approaches. One limits foreign customers of data brokers. The other adds export control limits on the export of certain personal data.<sup>67</sup>

The US has clearly shifted from being a country open to foreign investment in data-rich firms to one that views controlling data as essential to national security.

The US has clearly shifted from being a country open to foreign investment in data-rich firms to one that views controlling data as essential to national security. The US differs from India and China, however. There is no one law in the US which governs private sector use of personal data, but there are strong rules governing public sector use of citizens’ personal data. The amended Privacy Act of 1974 governs the collection, maintenance, use, and dissemination of information about individuals held by US government entities.<sup>68</sup>

### China: national security over commerce

China too has used national security as a rubric for controlling the practices of Chinese data-rich firms. When China's Data Security Law takes effect in September 2021, it will stipulate the following:

- Data collectors must obtain user consent to collect information and users have a right to withdraw that consent.
- Companies processing the data cannot refuse to provide services to users who do not consent to have their data collected,
- Firms must adhere to strict rules for transferring Chinese citizens' data outside the country, including getting government permission.
- Any company or person falling foul of the rules could be fined no more than 50 million yuan (US\$7.6 million), or 5 percent of the annual turnover.
- The state will establish a data protection structure and participate vigorously in international institutions to establish rules or norms for protecting personal data.<sup>69</sup>

According to an editorial in the *Global Times*, one purpose of Beijing's probe and punishment of Didi is to ensure the corporate sector does not own more data than the state.

The government's recent scrutiny of ride-sharing giant Didi Chuxing may be an indication of what lies ahead. According to an editorial in the *Global Times*, one purpose of Beijing's probe and punishment of Didi is to ensure the corporate sector does not own more data than the state.<sup>70</sup> Rather, the government seeks greater control over data-rich firms.

Not surprisingly, the Chinese government appears to be exempt from many of the law's provisions. According to China expert Jamie P. Horsley:

"Notice and consent is not required if laws require confidentiality or where it would impede performing their duties (Article 35) – situations that presumably would apply to national security and law enforcement matters."<sup>71</sup>

As with India, when Chinese officials mandate greater control of data, they do not subject the government to the limitations.

# Conclusion

Policymakers should create rules both to facilitate an appropriate enabling environment for data-driven growth and to protect their citizens and firms from harm.

Policymakers are just beginning to learn how to govern various types of data. According to the World Bank, policymakers should create rules both to facilitate an appropriate enabling environment for data-driven growth and to protect their citizens and firms from harm.

Under the guise of digital sovereignty, however, some governments are seeking to regulate commercial use of personal data without enacting clear rules governing the use of such data by the public sector. As the OECD has warned, these states may be using data governance to shift power from firms to government. Officials in these nations seem to believe that by controlling large supplies of data, they can achieve economic advantage in the digital economy and will be better positioned to counter the market power of the giant platforms.

Yet advocates of data sovereignty may be misguided. Researchers cannot yet ascertain if economics of scale and scope in data will yield competitive advantage. However, we do know that if nations or firms hoard data, they may reduce data generativity and the public benefits of data analysis.

Data has disrupted sectors from banking to tourism. Yet trade agreements could help policymakers address these disruptions and limit national efforts to over-control or hoard data. Policymakers could use trade agreements to develop more precise language that delineates how and when nations can use the exceptions, including the national security rationale, to limit cross-border data flows.

Secondly, multilateral organizations such as the OECD and the Asia Pacific Economic Cooperation (APEC) can gather governments into an international conference to develop global strategies for protecting personal data and consumer welfare. They can also encourage the United Nations Commission on International Trade Law (UNCITRAL) to create a model law that builds on principles drafted at the OECD and APEC as common ground. Nations could then adopt this model law to advance greater interoperability. With these steps, policymakers could boost trust in trade agreements as a tool to facilitate internationally accepted data governance rules.

Nonetheless, in the wake of the disruptions caused by data, expect more nations to claim that the best way to protect personal data is to control data.

# Researcher bio:

## Susan Ariel Aaronson

Susan Ariel Aaronson is Research Professor of International Affairs and Director of the Digital Trade and Data Governance Hub. Aaronson conceived of and directs the Hub, which aims to educate policymakers, the press and the public about domestic and international data governance issues from digital trade to public data governance.

Aaronson is also a Cross-Disciplinary Fellow and affiliate at George Washington University's Institute for International Economic Policy, the Institute for Science and Technology Policy and the Sigur Center. She is also a Senior Fellow at the think-tank Center for International Governance Innovation (GIGI) in Canada.

Aaronson is currently directing projects on mapping data governance; and writing on comparative advantage in data; trade as a tool to counter disinformation; data and national security, and America's approach to stimulating AI. Her research has been funded by the Hewlett, MacArthur, Koch, Ford, and Rockefeller Foundations; governments such as the Netherlands, US, and Canada; the UN, ILO, and World Bank, and US corporations including Ford Motor and Levi Strauss.

Previously, Aaronson was a Guest Scholar in Economics at the Brookings Institution (1995–1999); and a Research Fellow at the World Trade Institute 2008–2012. Aaronson was also the Carvalho Fellow at the Government Accountability Project and the Minerva Chair at the National War College.



**Susan Ariel Aaronson**

Research Professor, Cross-Disciplinary  
Fellow, and Director of the Digital Trade  
and Data Governance Hub,  
George Washington University;  
Senior Fellow, Centre for  
International Governance innovation

# Endnotes

1. Ravi Agrawal, "Why India and China are sparring", *Foreign Policy*, May 28, 2020, <https://foreignpolicy.com/2020/05/28/why-india-china-sparring-border-clashes-conflict/> and Anbarasan Ethirajan and Vikas Pandey, China-India border: Why tensions are rising between the neighbors, *BBC News*, June 2020, <https://www.bbc.com/news/world-asia-52852509> and [wdelhi/desai.pdf/](https://www.bbc.com/news/world-asia-52852509). More recently, see <https://asia.nikkei.com/Opinion/China-s-hostility-ensures-the-rise-of-a-more-antagonistic-India>
2. Lingling Wei, "China's new power play: More control of tech companies' troves of data," *The Wall Street Journal*, June 12, 2021, <https://www.wsj.com/articles/chinas-new-power-play-more-control-of-tech-companies-troves-of-data-11623470478>
3. Ibid. and *Bloomberg News*, "China blocks Didi from app stores days after mega US IPO"
4. Nayantra Ranganathan, "The seduction of data sovereignty in India," *Hindustan Times*, August 26, 2019, <https://www.hindustantimes.com/analysis/the-seduction-of-data-sovereignty-in-india/story-iOS8cVKxstlIgJLy47ly0J.html>
5. "India will allow data mobility only if reciprocated: Ravi Shankar Prasad", *The Economic Times*, June 15, 2019, <https://economictimes.indiatimes.com/tech/internet/india-will-allow-data-mobility-only-if-reciprocated-ravi-shankar-prasad/articleshow/69796915.cms>
6. Janosch Delcker, "Thierry Breton: European companies must be ones profiting from European data," *Politico*, January 19, 2020, <https://www.politico.eu/article/>; and EC, Thierry Breton, [https://ec.europa.eu/commission/commissioners/2019-2024/breton\\_en](https://ec.europa.eu/commission/commissioners/2019-2024/breton_en)
7. Treasury Board of Canada Secretariat, Government of Canada white paper: Data sovereignty and public cloud, 2018, <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/gc-white-paper-data-sovereignty-public-cloud.html#toc6>
8. Ibid.
9. Luciano Floridi, "The fight for digital sovereignty: What it is, and why it matters, especially for the EU", *Philosophy & Technology*, 33, 369–378 (2020), <https://doi.org/10.1007/s13347-020-00423-6>
10. House of Lords Covid 19 Committee, 1st Report Session 2021-22, "Beyond digital: the government responses", July 22, 2021, <https://committees.parliament.uk/publications/6880/documents/72531/default/>
11. This argument underpins the Biden Executive order on Competition. White House, "Executive Order on promoting competition in the American economy", July 9, 2021, <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/>. Also see Australia Productivity Commission, "Digital platforms inquiry final report", <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf>; Andrei Hagiu and Julian Wright, "When data creates competitive advantage and when it doesn't", *Harvard Business Review*, January/February 2020, <https://hbr.org/2020/01/when-data-creates-competitive-advantage>.
12. OECD, "Data driven innovation: Big data for growth and well-being", 2015, <https://www.oecd-ilibrary.org/docserver/9789264229358-en.pdf>
13. OECD, Working Party of the Trade Committee, "Digital trade inventory, Pillar I: rules, standards and principles", p.20, #69, April 14, 2021, [https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP\(2020\)14/FINAL&docLanguage=En](https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2020)14/FINAL&docLanguage=En)
14. WTO, "E-commerce negotiations advance, delve deeper into data flows," May 2021, [https://www.wto.org/english/news\\_e/news21\\_e/jsec\\_20may21\\_e.htm](https://www.wto.org/english/news_e/news21_e/jsec_20may21_e.htm). Also see Susan Ariel Aaronson and Thomas Struett, "Data is divisive: A history of public communications on e-commerce", 1998–2020, CIGI Paper No. 247, December 14, 2020, <https://www.cigionline.org/publications/data-divisive-history-public-communications-e-commerce-1998-2020/>
15. James Tebrake, Director General, Macroeconomic Accounts, Statistics Canada, "Capturing the digital economy in Canada's macroeconomic accounts" and Andreas Maurer, "Measuring digital trade – state of play", Geneva, 1 March 2018, <https://www.wto.org/>



- english/news\_e/news18\_e/1serv\_01mar18\_e.pdf
16. US Department of Commerce, "Measuring the value of cross-border data flows", 2016, <https://www.ntia.doc.gov/report/2016/measuring-value-cross-border-data-flows>; Jessica R. Nicholson and Ryan Noonan, "Digital economy and cross-border trade: The value of digitally-deliverable services," Washington, DC, US Department of Commerce, Economics and Statistics Administration, ESA Issue Brief #01-14, January 27, 2014, available at <http://www.esa.doc.gov/sites/default/files/digitaleconomyandcross-bordertrade.pdf>
  17. US Bureau of Economic Analysis, "Defining and measuring the digital economy: data tables" 1997-2017, April 2, 2019
  18. Ingo Borchert, Michael Gasiorek, Emily Lydgate, L. Alan Winters, "G7 leaders should discuss international trade (seriously)", Policy Brief 59, June 2021, University of Sussex, <https://blogs.sussex.ac.uk/uktpo/publications/g7-leaders-should-discuss-international-trade-seriously/>
  19. Susan Ariel Aaronson, "Data is different: Why the world needs a new approach to governing cross-border data flows," CIGI Paper No. 197, November 2018, pp. 5-7, <https://www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows/>
  20. <https://nic.org.uk/app/uploads/Data-As-Infrastructure.pdf>
  21. OECD, "Measuring data and data flows", <https://www.oecd.org/going-digital/mdt-roadmap-data.pdf>
  22. Carriere-Swallow & Haksar, "The economics and implications of data: An integrated perspective"
  23. Keith E. Maskus and Jerome H. Reichman, "The globalization of public knowledge goods and the privatization of global public goods," *Journal of International Economic Law* (2), 279-320; and OECD, "Economic and social benefits of internet openness," OECD Digital Economy Papers No. 257
  24. Charles I. Jones and Christopher Tonetti, "Nonrivalry and the economics of data", NBER Working Paper No. 26260 September 2019, revised April 2020 JEL No. E0, O4; Klievink, Bram, van der Voort, Haiko, and Veeneman, Wijnand, "Creating value through data collaboratives' information polity", vol. 23, no. 4, pp. 379-397, 2018; US Geological Service, "Why share your data?", <https://www.usgs.gov/products/data-and-tools/data-management/why-share-your-data>
  25. Elizabeth Dubois, Fenwick McKelvey and Taylor Owen, "What have we learned from Google's political ad pullout?", April 10, 2019, *Policy Options*, <https://policyoptions.irpp.org/fr/magazines/avril-2019/learned-googles-political-ad-pullout/>; and Robert Fay, Blayne Haggart, and Natasha Tusikov, "Reining in big tech: Is this the end of the beginning?", July 23, 2021, <https://www.cigionline.org/articles/reining-in-big-tech-is-this-the-end-of-the-beginning/>
  26. World Bank, "World development report 2016: Digital dividends", <https://www.worldbank.org/en/publication/wdr2016>
  27. World Bank, "World development report: Data for better lives, 2020", p. 2 <https://openknowledge.worldbank.org/bitstream/handle/10986/35218/211600mm.pdf>
  28. OECD, "Data-driven innovation," p. 18
  29. [www.statista.com/statistics/277483/market-value-of-the-largest-internet-companies-worldwide/](https://www.statista.com/statistics/277483/market-value-of-the-largest-internet-companies-worldwide/)
  30. 2021 data, <https://www.markinblog.com/largest-internet-companies/>. As of 2021, some 13 of these companies call the US home, nine are based in China and the other two are German and Japanese
  31. UNCTAD Secretariat, "Digital platforms and value creation in developing countries: Implications for national and international policies", February 19, 202, TD/B/EDE/4/2, #10, quote #14 p. 2
  32. W. van der Aalst, O. Hinz and C. Weinhardt, "Big digital platforms: growth, impact, and challenges", *Business & Information Systems Engineering*, 61, 645–648 (2019). <https://doi.org/10.1007/s12599-019-00618-y>
  33. UNCTAD Secretariat, "Digital platforms and value creation in developing countries: Implications for national and international policies", February 19, 202, TD/B/EDE/4/2, #10, quote #14 p. 2.
  34. Susan Ariel Aaronson, "Data Is different: Why the world needs a new approach to governing cross-border data flows", CIGI Paper No. 197, November 2018, <https://www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing->

- cross-border-data-flows/
35. Yan Carriere-Swallow & Vikram Haksar, 2019, "The economics and implications of data: an integrated perspective," IMF Departmental Papers / Policy Papers 2019/013, International Monetary Fund
  36. Amnesty International, "Surveillance giants: How the business model of Google and Facebook threatens human rights", November 21, 2019, <https://www.amnesty.org/en/documents/pol30/1404/2019/en/>
  37. Dipayan Ghosh, Lindsay Gorman, Bret Schafer, and Clara Tsao, "The weaponized web: Tech policy through the lens of national security," German Marshall Fund and Harvard Kennedy School, December 2020, <https://securingdemocracy.gmfus.org/wp-content/uploads/2020/12/The-Weaponized-Web.pdf>
  38. Dan Ciuriak, "The economics of data: Implications for the data driven economy", March 5, 2018 <https://www.cigionline.org/articles/economics-data-implications-data-driven-economy/> and Steven Weber, "Data Development and Growth", Business and Politics, 2017, Cambridge University Press, 19 (3) 411
  39. Teresa Scassa, "Rights in data, the public interest, and international trade law", Chapter in Ingo Borchert and L. Alan Winters, "Addressing impediments in digital trade", 2021, <https://voxeu.org/content/addressing-impediments-digital-trade>
  40. Office of the High Commissioner for Human Rights, "Disinformation and freedom of opinion and expression: Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and express", Irene Khan, 47th sess, A/HRC/47/25.
  41. National Intelligence Council, "Global trends 2040: A more contested world", 2021, pp. 48-49 [https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends\\_2040.pdf](https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf)
  42. NIST, "The unthinkable data challenge: Advancing methods in differential privacy", 2018, <https://www.nist.gov/ctl/pscr/open-innovation-prize-challenges/past-prize-challenges/2018-unlinkable-data-challenge>
  43. [https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en)
  44. Digital trade and data governance hub, Global data governance mapping project, 2020 data, <https://datagovhub.elliott.gwu.edu/2021/05/17/the-global-data-governance-mapping-project/>
  45. OECD, Working Party of the Trade Committee, "Digital trade inventory, Pillar I: rules, standards, and principles", p.20, #69, April 14, 2021, [https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP\(2020\)14/FINAL&docLanguage=En](https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2020)14/FINAL&docLanguage=En)
  46. Amanda Connolly, "Risks from Chinese takeovers mean Canada needs tougher investment rules: experts", *Global News*, 8 June 2020 at 5:02 PM, <https://globalnews.ca/news/7040029/canada-foreign-takeovers-china/>.
  47. Dan Ciuriak, "The WTO in the digital age", May 4, 2020, <https://www.cigionline.org/articles/wto-digital-age/>
  48. Susan Ariel Aaronson, "How nations can build online trust through trade", *Barron's*, May 4, 2021
  49. <https://www.dfat.gov.au/trade/services-and-digital-trade/australia-singapore-digital-economy-agreement-summary-key-outcomes>
  50. "Australia-Singapore digital economy cooperation on standards", Research Report, September 2020, p.3, [https://www.mti.gov.sg/-/media/MTI/Microsites/DEAs/Singapore-Australia-Digital-Economy-Agreement/SG-AU\\_Standards\\_for\\_Digital\\_Trade.pdf](https://www.mti.gov.sg/-/media/MTI/Microsites/DEAs/Singapore-Australia-Digital-Economy-Agreement/SG-AU_Standards_for_Digital_Trade.pdf)
  51. "G-7 roadmap for cooperation on data free flow with trust", April 28, 2021, [http://www.g8.utoronto.ca/ict/2021-annex\\_2-roadmap.html](http://www.g8.utoronto.ca/ict/2021-annex_2-roadmap.html). The G7 (or Group of Seven) is an organization made up of the world's seven largest so-called advanced economies: Canada, France, Germany, Italy, Japan, the United Kingdom and the United States, <https://www.bbc.com/news/world-49434667>
  52. Aaronson and Struett, "Data is divisive", pp 8-9. On Privacy Shield Negotiations, see Kenneth Propp, "Progress on transatlantic data transfers? The picture after the US-EU summit", June 21, 2021, <https://www.lawfareblog.com/progress-transatlantic-data-transfers-picture-after-us-eu-summit>
  53. WTO, Work Programme on Electronic Commerce, "The e-commerce moratorium: Scope and impact, communication from India and South Africa", WTO Doc WT/GC/W/798, online: WTO <[docs.wto.org](https://docs.wto.org)> [Scope and Impact]
  54. Steven Weber, "Data, development and growth", Business and Politics 19, (3):

- 397–423. [www.cambridge.org/core/services/aop-cambridge-core/content/view/DC04765FB73157C8AB76AB1742ECD38A/S1469356917000039a.pdf/data\\_development\\_and\\_growth.pdf](https://www.cambridge.org/core/services/aop-cambridge-core/content/view/DC04765FB73157C8AB76AB1742ECD38A/S1469356917000039a.pdf/data_development_and_growth.pdf)
55. UNCTAD, “Information economy report 2017: Digitalization, trade and development”, [https://unctad.org/en/PublicationsLibrary/ier2017\\_overview\\_en.pdf](https://unctad.org/en/PublicationsLibrary/ier2017_overview_en.pdf).
  56. Viktoriya Gusevva, “Understanding data sovereignty”, *In County*, November 14, 2020, <https://incountry.com/blog/understanding-data-sovereignty/>
  57. Dashveenjit Kaur, “India’s new social media rules explained,” *Techwire Aisa*, June 1, 2021, <https://techwireasia.com/2021/06/indias-new-social-media-rules-explained/>; Joseph Menn, “WhatsApp sues Indian government over new privacy rules – sources”, *Reuters*, May 26, 2021, <https://www.reuters.com/world/india/exclusive-whatsapp-sues-india-govt-says-new-media-rules-mean-end-privacy-sources-2021-05-26/>
  58. Talwar Thakore & Associates, Linklaters, “Data protected - India”, March 2020, <https://www.linklaters.com/en/insights/data-protected/data-protected---india>
  59. <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-india-technology-to-transform-a-connected-nation>
  60. Susan Ariel Aaronson, “Data is a development issue”, CIGI Papers No. 223 — July 2019, p. 3
  61. “Privacy and Data Protection – India Wrap 2020”, *The National Law Review*, January 15, 2021, <https://www.natlawreview.com/article/privacy-and-data-protection-india-wrap-2020>
  62. “India will allow data mobility only if reciprocated: Ravi Shankar Prasad”, 2019, *The Economic Times*, <https://economictimes.indiatimes.com/tech/internet/india-will-allow-data-mobility-only-if-reciprocated-ravi-shankar-prasad/articleshow/69796915.cms>; and Tricia Ray, “The encryption debate in India: 2021 update”, 2021, Carnegie Endowment, <https://carnegieendowment.org/2021/03/31/encryption-debate-in-india-2021-update-pub-84215>
  63. See [www.treasury.gov/resource-center/international/Documents/Summary-of-FIRMA.pdf](https://www.treasury.gov/resource-center/international/Documents/Summary-of-FIRMA.pdf)
  64. White House, 2019, “Executive Order on securing the information and communications technology and services supply chain”, May 15, <https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/>
  65. The final regulations are available at <https://s3.amazonaws.com/public-inspection.federalregister.gov/2020-00188.pdf>
  66. <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/>
  67. Senator Ron Wyden, <https://www.wyden.senate.gov/news/press-releases/wyden-releases-draft-legislation-to-protect-americans-personal-data-from-hostile-foreign-governments>
  68. US Department of Justice, Privacy Act, <https://www.justice.gov/opcl/privacy-act-1974>
  69. “China’s draft ‘Personal Information Protection Law’” (full translation), DigiChina Project, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-draft-personal-information-protection-law-full-translation/>
  70. Hunton Williams Kurth, “China issues data security law”, *National Law Review*, June 16, 2021, <https://www.natlawreview.com/article/china-issues-data-security-law>; and Masha Borak, “Why is Didi’s cybersecurity review important and what will it mean for the ride-hailing giant’s future?”, *South China Morning Post*, July 5, 2021, <https://www.scmp.com/tech/big-tech/article/3139888/why-didis-cybersecurity-review-important-and-what-will-it-mean-ride>
  71. Jamie P. Horsley, “How will China’s privacy law apply to the Chinese state?”, Brookings Institution, January 29, 2021, <https://www.brookings.edu/articles/how-will-chinas-privacy-law-apply-to-the-chinese-state/>

---

The Hinrich Foundation is a unique Asia-based philanthropic organization that works to advance mutually beneficial and sustainable global trade.

We believe sustainable global trade strengthens relationships between nations and improves people's lives.

We support original research and education programs that build understanding and leadership in global trade. Our approach is independent, fact-based and objective.

---

#### MEDIA INQUIRIES





Ms. Theresa Fonseca,  
Head of Marketing and Communications  
T: +65 6982 6816  
[theresa.fonseca@hinrichfoundation.com](mailto:theresa.fonseca@hinrichfoundation.com)

There are many ways you can help advance sustainable global trade. Join our training programs, participate in our events, or partner with us in our programs. [inquiry@hinrichfoundation.com](mailto:inquiry@hinrichfoundation.com)

Receive our latest articles and updates about our programs by subscribing to our newsletter

[hinrichfoundation.com](https://hinrichfoundation.com)



 [hinrichfdn](https://twitter.com/hinrichfdn)  
 [hinrichfoundation](https://facebook.com/hinrichfoundation)  
 [hinrich foundation](https://linkedin.com/company/hinrich-foundation)  
 [hinrichfoundation](https://youtube.com/hinrichfoundation)

#### Disclaimer:

The Hinrich Foundation is a philanthropic organization that works to advance mutually beneficial and sustainable global trade through original research and education programs that build understanding and leadership in global trade. The Foundation does not accept external funding and operates a 501(c)(3) corporation in the US and a company in Singapore exclusively for charitable and educational purposes. © 2021 Hinrich Foundation Limited. See our website [Terms and Conditions](#) for our copyright and reprint policy. All statements of fact and the views, conclusions and recommendations expressed in the publications of the Foundation are the sole responsibility of the author(s).