THE NATIONAL INTEREST

The Danger of Blindly Navigating Data Nationalism

Simon Lester and Huan Zhu

February 21, 2021

Digital trade and the flow of digital information are certain to grow in prominence in the future. The coronavirus pandemic has pushed their growth curve along.

Recently, a "consolidated negotiating text" for the e-commerce negotiations at the World Trade Organization was leaked. What this text shows is that while progress has been made, there is still a lot of work to do. The text "consolidates" the various viewpoints of the negotiating governments by collecting them all in one document, and it is clear that there are many issues on which these governments do not agree, including the fundamental issue of rules on data flows.

Despite these differences, this project needs to continue. As the importance of data grows in both the commercial and regulatory arenas, the need for broadly applicable international norms to guide businesses and governments becomes ever greater. Many companies with a digital focus rely on data as part of their business model, while governments are increasingly worried about the privacy and security issues that arise as a result. But what business practices are acceptable? And what are the limits of appropriate governmental regulation? Unfortunately, international rules in this area are underdeveloped and do not adequately address these issues. This needs to change soon in order to avoid geopolitical conflict and protectionism. This needs to change in order to ensure that businesses know the rules of the road.

Currently, we are at about the same stage on data flows that we were for trade in goods before World War II. At that time, there were a number of bilateral trade agreements dealing with goods, but no comprehensive multilateral rules. As a result, there was no overarching framework under which businesses and governments could operate. Even when the General Agreement on Tariffs and Trade (GATT), the first multilateral trade agreement, took effect in 1948, there was uncertainty about what the rules meant. There were words on paper, but it was not clear what impact they would have on actual trade flows. The nuances of the rules were only sorted out after decades of experience with discussions and disputes at the GATT and then the World Trade Organization (WTO), its successor organization.

Now we have the same problem with digital rules. There are some bilateral and regional rules on data that have been pushed by the United States, as well as by the European Union and other countries. But these are competing international frameworks, rather than a comprehensive multilateral solution. In addition, these rules have not been tested and most people have little

sense of what they mean. The lack of clarity means uncertainty for both businesses and regulators.

Munich Conference Exposes the Decline of the West

To take an example from the U.S. agreements on digital trade, there are some broad obligations in the United States-Mexico-Canada Agreement (USMCA) related to the flow of cross-border data. At the same time, there are also multiple exceptions to the obligations. There is a specific exception to the cross-border data provision for government measures that are "necessary to achieve a legitimate public policy objective." There are general exceptions for certain designated public policy objectives, which apply to all obligations in the agreement. Additionally, there are extremely deferential "security" exceptions that could come up if governments restrict data flows due to concerns about cybersecurity.

The problem is, when these obligations and exceptions are considered together, it is not clear what impact these agreements have on actual data restrictions imposed by governments in the real world. Nevertheless, it is important to start somewhere, and, as with trade in goods, the specific meaning of the rules will have to be fleshed out through implementation and enforcement.

The foreign trade agreements (FTA) of other countries are also instructive. European Union-led FTAs have less extensive obligations and tend to focus on privacy protection. For example, the chapter on e-commerce in the Canada-EU trade agreement is fairly limited in scope. It promotes issues such as data privacy and has general exceptions that allow parties to take measures inconsistent with the agreement in order to protect public security and privacy. Similarly, the EU-Japan Economic Partnership Agreement does not require free data flow, only stating that parties will "reassess within three years" whether provisions of this type should be included. For now, the EU considers personal data to be a human rights issue and only allows data outflow under certain circumstances, including through adequacy decisions, certification mechanism, standard contractual clauses and other means. It could be a challenge to convince the EU to make significant commitments on data flows in a multilateral setting.

China is even more of a challenge. As a growing geopolitical rival, China presents a different set of concerns. Current Chinese law establishes the principle of cyber sovereignty and imposes certain restrictions on data flows (both inward and outward) for security reasons. These restrictions have led China to avoid strong data rules in its FTAs. For instance, China's FTAs with South Korea and Australia, as well as the recent China-New Zealand FTA upgrade, all focus on data protection when it comes to rules on data. On the other hand, the Regional Comprehensive Economic Partnership (RCEP), negotiated by China and fourteen other countries (but not yet ratified), could, in theory, move China in the direction of being more amenable to data flows. Along the lines of the language in USMCA, RCEP has language that ensures the cross-border transfer of information, while providing exceptions for "legitimate public policy objectives" and "essential security interests." However, many observers are skeptical that this will lead to any change in China's practices in this area.

Beyond the efforts of these larger economies, a group of smaller countries has also been trying to develop new rules in this area. Chile, New Zealand, and Singapore have recently signed the Digital Economic Partnership Agreement (DEPA), which has cutting-edge provisions in a number of areas related to digital trade. The DEPA takes an approach to data flows which is

similar to that of the U.S. agreements, with broad obligations to allow data flows, which are then qualified by exceptions.

Turning to the multilateral efforts, negotiating progress at the WTO has been slow, in part because each country has its own priorities in the negotiations. In addition, certain countries have serious concerns, even distrust, over cybersecurity that prevent them from making broad commitments on data flows with each other. The United States and China are the prime example of this tension.

Despite the difficulties, the issues are too important to ignore. Bilateral agreements between like-minded countries are of only limited value. Ultimately, if there is to be a coherent set of multilateral rules, then all the major players will have to sit down and work out a compromise. Carveouts of sensitive areas can be used in order to reach an agreement if necessary, but the core issues here need multilateral disciplines.

Digital trade and the flow of digital information are already enormous, and they are certain to grow in prominence in the future. The pandemic has pushed the growth curve along. In order to manage trade conflict in this area, multilateral rules must be developed—rules that are clear and well-understood. The sooner the process moves forward, the sooner there will be a useful framework to guide businesses and governments.

Simon Lester is associate director of the Herbert A. Stiefel Center for Trade Policy Studies at the Cato Institute.

Huan Zhu is a research associate at the Cato Institute's Herbert A. Stiefel Center for Trade Policy Studies.